PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-138667
(43)Date of publication of application : 16.05.2000

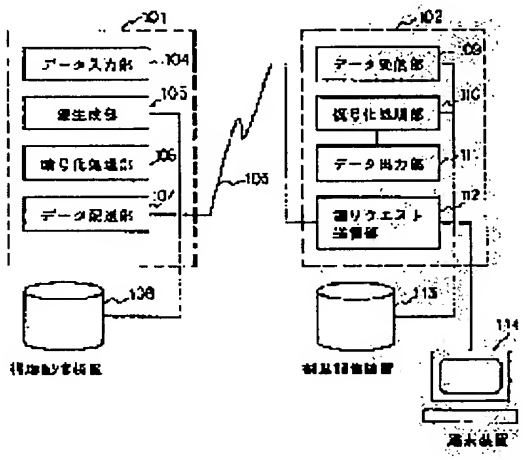
(51)Int.Cl. H04L 9/14
G06F 12/14
G09C 1/00

(21)Application number : 11-338145
(22)Date of filing : 10.02.1994

(71)Applicant : HITACHI SOFTWARE ENG CO LTD
(72)Inventor : TAGO SHIGERU

(54) METHOD AND SYSTEM FOR CONTROLLING CIRCULATION DATA REFERENCE ORDER

(57)Abstract:
PROBLEM TO BE SOLVED: To reference circulation data in the order in response to the reference order of data users without making processing by a circulation data server complicated.
SOLUTION: A circulation data server side device 101 generates cryptographic keys whose number is the same number as a reference right order number set to a circulation data set consisting of plurality of partial data, transfers the data to the device of a circulation data user, which adds an encrypted partial data set resulting from encrypting all partial data that are referenced by users with next and succeeding ranking reference right by cryptographic key corresponding to the reference right order to specific partial data corresponding to one reference right order, and conducts the processing encrypting a data set consisting of the specific partial data and the encrypted partial data set by using the cryptographic key corresponding to the reference right order for the same number of times as the reference right order number, a user side device 102 acquires the encrypted circulation data set in response to a request from the user, demodulates the corresponding partial data by using the cryptographic key corresponding to the reference right order of the user and provides an output of the decoded data in a form that can be referenced by the data users.



CLAIMS

[Claim(s)]

[Claim 1]A control method of the order circulating data reference characterized by comprising the following.
Inside of a circulating data set which comprises two or more piece data provided by the circulating data donor side device, It is the control method of the order circulating data reference which enables reference of specific piece data of reference authority ranking which a user of the circulating data user side device demands on condition that all the users who have the reference authority ranking of a higher rank rather than the user concerned are ending with reference, A step which generates or sets up an encryption key of the number of reference authority ranking and the same number which were set up to a circulating data set which comprises two or more piece data in the circulating data donor side device, and is transmitted to the circulating data user side device.
An encryption partial data set which enciphered all the piece data referred to by a user of reference authority after the following ranking with an encryption key corresponding to the reference authority ranking is added to specific piece data corresponding to one reference authority ranking, Processing which enciphers a data set which comprises these specific piece data and an encryption partial data set with an encryption key corresponding to the reference authority ranking concerned, In a step which the number of reference authority ranking and a number-of-times line of said encipher the whole data set, and stores this enciphered circulating data set in memory storage, and the circulating data user side device, A circulating data set stored in said memory storage is acquired according to a demand from a circulating data user, A step which re-stores the encryption piece data concerned in said memory storage when decode piece data corresponding with an encryption key corresponding to reference authority ranking of the user concerned, and it outputs in form which a data user can refer to and encryption piece data exists in decoded piece data.

[Claim 2]Inside of a circulating data set which comprises two or more piece data provided by the circulating data donor side device characterized by comprising the following, The order control system of circulating data reference which enables reference of specific piece data of reference authority ranking which a user of the circulating data user side device demands on condition that all the users who have the reference authority ranking of a higher rank rather than the user concerned are ending with reference.
An encryption key creating means which, as for said circulating data donor side device, generates or sets up an encryption key of the number of reference authority ranking and the same number which were set up to a circulating data set which comprises two or more piece data, and is transmitted to the circulating data user side device.
An encryption partial data set which enciphered all the piece data referred to by a user of reference authority after the following ranking with an encryption key corresponding to the reference authority ranking is added to specific piece data corresponding to one reference authority ranking, Processing which enciphers a data set which comprises these specific piece data and an encryption partial data set with an encryption key corresponding to the reference authority ranking concerned, The number of reference authority ranking and a number-of-times line of said encipher the whole data set, possess an encryption processing means to store this enciphered circulating data set in memory storage, and it said circulating data user side device, A circulating data set stored in said memory storage is acquired according to a demand from a circulating data user, A decoding processing means to re-store the encryption piece data concerned in said memory storage when decode piece data corresponding with an encryption key corresponding to reference authority ranking of the user concerned, and it outputs in form which a data user can refer to and encryption piece data exists in decoded piece data.

[Claim 3]A control method of the order circulating data reference characterized by comprising the following.
Inside of a circulating data set which comprises two or more piece data provided by the circulating data donor side device,

It is the control method of the order circulating data reference which enables reference of specific piece data of reference authority ranking which a user of the circulating data user side device demands on condition that all the users who have the reference authority ranking of a higher rank rather than the user concerned are ending with reference, A step which generates or sets up an encryption key of the number of reference authority ranking and the same number which were set up to a circulating data set which comprises two or more piece data in the circulating data donor side device, and is transmitted to the circulating data user side device.
Specific piece data corresponding to the lowest reference authority ranking is enciphered with an encryption key corresponding to the reference authority ranking concerned, Piece data which a user of reference authority ranking of one higher rank can refer to is added to this encryption piece data, Processing which enciphers these encryption piece data and piece data of reference authority ranking of one higher rank with an encryption key corresponding to reference authority ranking of one higher rank, In a step which stores an enciphered circulating data set in memory storage repeatedly until encryption of piece data in the top reference authority ranking is completed, and said circulating data user side device, A circulating data set stored in said memory storage is acquired according to a demand from a circulating data user, A step which re-stores the encryption piece data concerned in said memory storage when decode piece data corresponding with an encryption key corresponding to reference authority ranking of the user concerned, and it outputs in form which a data user can refer to and encryption piece data exists in decoded piece data.

[Claim 4]Inside of a circulating data set which comprises two or more piece data provided by the circulating data donor side device characterized by comprising the following, The order control system of circulating data reference which enables reference of specific piece data of reference authority ranking which a user of the circulating data user side device demands on condition that all the users who have the reference authority ranking of a higher rank rather than the user concerned are ending with reference.
An encryption key creating means which, as for said circulating data donor side device, generates or sets up an encryption key of the number of reference authority ranking and the same number which were set up to a circulating data set which comprises two or more piece data, and is transmitted to the circulating data user side device.
Specific piece data corresponding to the lowest reference authority ranking is enciphered with an encryption key corresponding to the reference authority ranking concerned, Piece data which a user of reference authority ranking of one higher rank can refer to is added to this encryption piece data, Processing which enciphers these encryption piece data and piece data of reference authority ranking of one higher rank with an encryption key corresponding to reference authority ranking of one higher rank, It repeats until encryption of piece data in the top reference authority ranking is completed, Provide an encryption processing means to store an enciphered circulating data set in memory storage, and said circulating data user side device, A circulating data set stored in said memory storage is acquired according to a demand from a circulating data user, A decoding processing processing means to re-store the encryption piece data concerned in said memory storage when decode piece data corresponding with an encryption key corresponding to reference authority ranking of the user concerned, and it outputs in form which a data user can refer to and encryption piece data exists in decoded piece data.

[Translation done.]

DETAILED DESCRIPTION

[Detailed Description of the Invention]
[0001]
[Field of the Invention]This invention relates to the control method of the order reference of circulating data and system in the system which refers to the circulating data set provided by the circulating data donor by the circulating data user side, It is related with the control method of the order circulating data reference and system which enable the reference of the specific piece data of the reference authority ranking which the user of circulating data demands especially on condition that all the users who have the reference authority ranking of a higher rank rather than the user concerned are ending with reference.
[0002]
[Description of the Prior Art]In the system which provides a data user with a certain data, and makes it refer to it one by one from a donor, There is a case where he would like to limit what can be referred to among two or more piece data according to the stage of performing processing which divides the data into two or more piece data and in which a data user refers to data by the demand by the side of a data donor. For example, it may be contractually said till a certain point in time that a data user is allowed to refer to only a specific portion among all the data, and reference of all the data will be allowed if it passes over the time. After the ranges of data to refer to for every data user differed or referring to it to a certain range, in order to use the data to be used as more detailed data, carry out additional fee collection to come to refer to the data of the still more detailed range when a certain pay data is distributed freely, but. It may be referred to as liking to protect to use more detailed data by the fee collection only for this addition. Or the 1st data user who received offer of data first may be allowed to refer to only a specific portion among all the data, the data of all the may be relayed to the 2nd next data user, and it may be told to the 2nd data user that reference of all the data is allowed.
[0003]In order to realize such a thing, there is the following art conventionally.
(1) Don't provide a data user with all the data in one procedure, but provide the piece data whose reference is enabled one by one according to a data user's demand.
(2) Divide data into two or more piece data, encipher each with a different encryption key, and provide for a data user. Henceforth, according to a data user's demand, the decode key of the piece data whose reference is enabled is provided one by one.
[0004]
[Problem(s) to be Solved by the Invention]However, there are the following problems by these methods.
(1) In the stage with which a data user is provided from a data donor, a certain piece data. When it is considered as the conditions which enable the reference of that piece data and it is required that a data user should be ending with reference about another piece data, after managing whether the data user fulfills this condition by the data donor side, it is necessary to judge whether the target piece data is provided. For that purpose, it is necessary to be related with all the data users and all the piece data, to obtain or hold the information whether the reference process of each piece data was performed, and to manage it by whether the data user was provided with each piece data in the past, and a data user. As a result, the processing by the side of a data donor becomes very complicated.
[0005](2) When reference of the piece data which changes with two or more data users especially is permitted, Under the demand of becoming possible to refer to the piece data in which another data user (the 2nd data user) corresponds after referring to the piece data in which a certain data user (the 1st data user) corresponds, by the data donor side. After checking having referred to the piece data in which the 1st data user corresponds, offer of the decode key with which piece data provides or corresponds to the 2nd data user must be performed, and the processing by the side of a data donor becomes very complicated.
[0006]The purpose of this invention, without making complicated processing by the side of a data donor, It is providing the

control method of the order circulating data reference and system which enable the reference of the specific piece data of the reference authority ranking which the user of circulating data demands on condition that all the users who have the reference authority ranking of a higher rank rather than the user concerned are ending with reference.

[0007]

[Means for Solving the Problem]To achieve the above objects, fundamentally, this invention is characterized by comprising the following, in order to enable reference of specific piece data of reference authority ranking which a user of circulating data demands, on condition that all the users who have the reference authority ranking of a higher rank rather than the user concerned are ending with reference.

A step which generates or sets up an encryption key of the number of reference authority ranking and the same number which were set up to a circulating data set which comprises two or more piece data in the circulating data donor side device, and is transmitted to the circulating data user side device.

An encryption partial data set which enciphered all the piece data referred to by a user of reference authority after the following ranking with an encryption key corresponding to the reference authority ranking is added to specific piece data corresponding to one reference authority ranking, A step which the number of reference authority ranking and a number-of-times line of said encipher processing which enciphers a data set which comprises these specific piece data and an encryption partial data set with an encryption key corresponding to the reference authority ranking concerned for the whole data set, and stores this enciphered circulating data set in memory storage.

In the circulating data user side device, a circulating data set stored in said memory storage is acquired according to a demand from a circulating data user, A step which re-stores the encryption piece data concerned in said memory storage when decode piece data corresponding with an encryption key corresponding to reference authority ranking of the user concerned, and it outputs in form which a data user can refer to and encryption piece data exists in decoded piece data.

[0008]In a circulating system which according to the above-mentioned means relays data among two or more data users, and permits reference of piece data in order, Decryption and a reference process of reference part data applicable by the 2nd user of the following ranking only after decryption and a reference process of reference part data applicable by the 1st data user who has the top reference authority ranking are performed become possible. Namely, when you would like to refer to your circulating data, [who has a data user among circulating data provided from the circulating data donor side] It becomes conditions to refer to circulating data which all the users who have the reference authority ranking of a higher rank rather than their reference authority ranking should refer to, Only when this condition is fulfilled, circulating data in which he has reference authority can be referred to, and it can guarantee referring to circulating data in order of reference authority.

[0009]Therefore, offer of an encryption key for corresponding decoding to the 2nd data user from a circulating data donor, It becomes possible not to be because decryption and a reference process of reference part data of the 1st data user who has the top reference authority ranking to be executed, but to carry out, Since it becomes unnecessary to check execution of decryption and a reference process the 1st data user's reference part data by the data donor side, turn of a reference process of the 1st data user and the 2nd data user can be checked easily.

[0010]

[Embodiment of the Invention]Hereafter, an embodiment of the invention is described according to a drawing.

(Embodiment 1) By a data donor, broadly, distribute data to many and unspecified data users, and by a data user's hope. The embodiment of the data multi stage story reference system which carries out additional fee collection of the range of the data whose reference is attained among the distributed data in the form which is changed into a large thing and added from a narrow thing to the contents of fee collection over the narrow referred data range in that case is described. If this system has the volition of getting a user to try only some of functions and picture data of game software first, and liking to enjoy the whole game succeedingly as a distribution system of game software for example, to a user, It is applied, when saying that use of the whole game is allowed because I have a surcharge to it paid.

[0011]Drawing 1 is a system configuration figure showing one embodiment of such a system. In drawing 1, the network which 101 connects the computer system by the side of a data donor, 102 connects the computer system by the side of a data user, and 103 connects the computer systems 101 and 102, and transmits data, and 104 are data input parts which input the data provided from the data donor side. This data input part 104 comprises a keyboard, a mouse, a microphone, a video photographing machine, etc. The enciphering processing part which performs a data encryption using the encryption key with which 105 was generated by the encryption key generation part and 106 was generated by the encryption key generation part 105, The data delivery part which performs processing whose 107 transmits the data enciphered by the enciphering processing part 106 to the computer system 102 by the side of a user via the network 103,

and 108 are auxiliary storage units which remember the key group generated by the key generation part 105. The data receiving section which receives the data in which 109 has been transmitted via the network 103, The decoding processing part which performs processing whose 110 decrypts code data with an encryption key, and 111 are data output parts which output the data decrypted by the decoding processing part 110, and this data output part 11 comprises a display, a loudspeaker, a printer, etc.

[0012]The key request transmission part which transmits the key request required as 112 transmitting the encryption key used for decoding of code data to a data donor via the network 103 (encryption key acquisition means), The auxiliary storage unit with which 113 memorizes the data distributed by the data donor, and 114 are terminal units which input a command for a data user to transmit a key request.

[0013]Drawing 2 is a lineblock diagram of the table 200 which records the range over all the data of each piece data when the whole data which a data donor provides is divided into two or more piece data, and comprises the three storage areas 201,202,203 for every piece data. Among these, the area which stores the ID number to which the storage area 201 was assigned to each divided piece data, The area where 202 stores the offset value from the initial data of all the data to the initial data of applicable piece data, and 203 are area which stores the size (data size) of each piece data.

[0014]The table 300 which records the classification at the time of gathering two or more piece data made possible [reference by different fee collection in relation to the charging method in this embodiment] for drawing 3 as a piece data group is shown, The area 301 which stores the consecutive numbers of a piece data group, and the area 302 which stores the ID number of the piece data contained in an applicable piece data group are comprised. The example of drawing 3 shows the relation between consecutive numbers when the piece data group 1 comprises the piece data 1, 3, 6, and 7, and a piece data ID number.

[0015]Drawing 4 showed the table 400 which stores the encryption key which uses each piece data group for enciphering and decrypting, and is provided with the area 401 which stores the consecutive numbers of a piece data group, and the area 402 which stores the encryption key data corresponding to the consecutive numbers.

[0016]To the piece data group which shows the table 500 which stores the frame by which additional fee collection is carried out in order to refer to each piece data group, and is shown with the consecutive numbers 501, drawing 5 is provided with the area 502 which stores the frame by which additional fee collection is carried out, in order to refer to it.

[0017]The area 601 which drawing 6 shows the table 600 which stores the total of the charge amount charged at each data user, and stores data user ID, such as each data user's bank account number, and ID of a driver's license, The area 602 which stores the total of the charge amount to the data come to hand and referred to from the data donor in the past according to a data user is formed.

[0018]Drawing 7 and drawing 8 are flow charts which show the flow of processing of this embodiment. Hereafter, operation is explained according to this flow chart. First, provision data is inputted from the data input part 104 by the data donor side, and the range of the piece data divided and divided into piece data by the difference in the charge amount for reference of this is stored in the table 200 of drawing 2 (Step 701). Next, with the same charge amount, the piece data whose reference is attained is gathered, and it is considered as a piece data group, and stores in the table 300 of drawing 3 (Step 702). This table 300 can refer [the data user] now all piece data groups applicable by paying a certain surcharge.

[0019]Here, although it is that to which it ranked with the piece data 1 and 2 and 3 -- in order of the reference, and it was located in a line with the condition --, in order of consecutive numbers, piece data is gathered so that it may belong to the piece data group from which the piece data referred to this time and the piece data referred to next differ, when collecting as a piece data group.

[0020]Next, the number of piece data groups and the encryption key for the same number which were carried out in this way and created are created by the key generation part 105 (Step 703). In this case, it is desirable for all the keys to differ. The encryption key group generated here is memorized by the auxiliary storage unit 108 (Step 704). Next, processing which enciphers the data with which a user is provided is performed. First, final charge amount enciphers the piece data group which should be decrypted at the end most greatly by one of the encryption keys, The consecutive numbers of the enciphered piece data group are stored in the consecutive-numbers storage area corresponding to the encryption key used this time among the piece data group consecutive-numbers storage areas 401 of the table 400 of drawing 4 (Step 705).

[0021]Next, the piece data group decrypted by the decoding processing before [one] decrypting this piece data group, and the data enciphered at Step 705 are connected, and 1 set of data is created (Step 706). Step 705 enciphers the merge data created here with another encryption key, and the consecutive numbers of the enciphered piece data group are stored in the consecutive-numbers storage area corresponding to the encryption key used among the consecutive-

numbers storage areas 401 of the table 400 of drawing 4 this time (Step 707). Next, the piece data group further decrypted by the decoding processing before one more and the data enciphered at Step 707 are connected, and 1 set of data is created (Step 706). Henceforth, this is repeated until it finishes enciphering all the piece data groups of provision data (Step 708).

[0022]For example, as shown in drawing 9, supposing provision data is divided into the four piece data groups 901-904, at first, It is enciphered by the encryption key K4 with which the piece data group 904 whose reference is attained corresponds to the last, and next, the encryption data 904S is added to the piece data group 903 referred to one step ago, and it is enciphered by the encryption key K3 with which these piece data group 903 and the encryption data 904S correspond.

[0023]Next, the encryption data 903S is similarly added to the piece data group 902 referred to one step ago, and it is enciphered by the encryption key K2 with which these piece data group 902 and the encryption data 903S correspond. Finally the encryption data 902S is added to the piece data group 901 referred to one step ago, and it is enciphered by the encryption key K2 with which these piece data group 901 and the encryption data 902S correspond.

[0024]Thus, the provision data which encryption ended is transmitted to the computer system 102 by the side of a data user by the data delivery part 107 via the network 103 (Step 709). At this time, the contents of the table 200,300 of drawing 2 and drawing 3 are also transmitted simultaneously. The method of transmission can consider how to receive the transfer request beforehand and transmit [I save at the sharable auxiliary storage unit, and have transmitted arbitrarily, or] to each user individually etc. The encryption provision data transmitted to the computer system 102 by the side of a user and the data of the table 200,300 are memorized by the auxiliary storage unit 112 by the side of a data user (Step 710). After this time, the data user can acquire now the encryption key for decrypting the piece data group of the range to refer to from a data donor in exchange for that price.

[0025]Here, the example to which the range of the data which can be referred to to what has large charge amount is expanded one by one is explained after referring to what has small charge amount. The method of acquiring two or more encryption keys by one processing can be realized similarly to refer to two or more piece data groups of a fixed range from the start.

[0026]First, in order to refer to the first piece data group, a data user inputs a key request SEND statement from the terminal unit 115, and makes a key request transmit to the data donor side via the network 103 by the key request transmission part 114 (Step 711). Under the present circumstances, with reference to the contents of the table 300 of drawing 3, the ID number of the piece data group of reference hope is transmitted simultaneously. The computer system 101 of the data donor who received the key request, The charge amount of a piece data group which received the key request from the table 500 of drawing 5 is searched, and the frame is added to the present amount of the total of the total study storage area corresponding to the data user who transmitted the key request among the amount storage areas of the total of the table 600 of drawing 6 (Step 712).

[0027]Then, the data of an encryption key when the piece data group which received the request is enciphered is transmitted to the data user side (Step 713). The decoding processing part 110 of the computer system 102 by the side of the data user who received encryption key data decrypts the whole code data which contains the piece data group of reference hope using the transmitted encryption key data (Step 714). Next, since the piece data group comprises two or more piece data, the data output part 111 reconstructs an order of the piece data belonging to a different piece data group based on the contents of the table 200,300 of drawing 2 and drawing 3 (Step 715).

[0028]Next, confirm whether the data output part 111 is a format in which the output of the reconstructed data is possible (Step 716), and when an output is not possible, . There is no data user who tried to perform this reference process in the stage where reference of applicable piece data is allowed. That is, from applicable piece data, it judges that the regular reference process to the piece data which must be referred to before has not performed yet, and a data user is notified of that from the terminal unit 114 (Step 718). When you wish reference of piece data applicable when a data user refers to the piece data in a succeedingly just order, transmission of an applicable just key request is re(Step 719) performed. The whole processing is ended when a data user does not have the volition which redoes processing of a just order like [when it is going to refer to unjustly applicable piece data].

[0029]When it is judged at Step 716 that it is the format in which an output is possible, the reconstructed data is outputted in the form where the utilizing method of data was balanced (Step 716). Here, when operation of the purport that the following piece data group is referred to further is performed by the terminal unit 114, it returns from Step 720 to Step 711, and the above processing is repeated and is performed. It can be gradually referred to one by one to the range which wishes the piece data group currently prepared by this into the data which a data donor provides.

[0030]Namely, according to the table 300 of drawing 3, as a piece data group referred to first, Since the piece data 1, 3, 6,

and 7 is assigned and the piece data 2 and 4 and -- are assigned as a piece data group referred to at the following stage, When the encryption key corresponding to regular reference stage turn is acquired and provision data is decoded with this encryption key, in the first reference stage 1. As a white frame shows to drawing 10, only the piece data 1, 3, 6, and 7 is decoded, it is outputted in the form which can be referred to to a user, and the piece data 2 and 4 is outputted in the following reference stage 2 in the form which can further be referred to. And in the following reference stage 3, the piece data 5 is outputted in the form which can further be referred to. It can be gradually referred to one by one to the range which wishes a piece data group by this repetition.

[0031]However, since the piece data group 1 is not yet decoded when the encryption key corresponding to the following piece data group 2 tends to refer provision data with reference to the piece data group 1 to the beginning, the piece data group 2 cannot be decoded. Therefore, preventing decrypting piece data to refer to at a present stage, without omitting a reference process one step ago unjustly, or receiving offer of the encryption key corresponding to the reference process one step before a data donor can be realized easily.

[0032]When circulating data between (Embodiment 2), next two or more users, the embodiment of a system which operates the circulation order is described. For example in the document exchanged in the company, such a system is applied, when there is a circulation thing which the manager needs to force so that a section chief may be read rather than a chief and reference authority ranking may read the document sequentially from the person of a higher rank namely, previously rather than a section chief.

[0033]Drawing 11 shows the system configuration of this embodiment, and 801 is a network which performs data transfer. 802 (A), 803 (B), 804 (C), 805(X), and 816 (Y) are computers which perform the same processing as the computer system 101,102 shown in Embodiment 1. 807 is an input device which inputs the data to circulate. 808 is an auxiliary storage unit which memorizes two or more encryption keys, and is connected to the computer 806 (Y). It is the shared auxiliary storage unit which 809 memorizes code data and can be accessed from each user.

[0034]Drawing 12 shows the composition of the code data circulated by this embodiment. 901-903 are circulating data referred to by different user, respectively, and it is data in which the 1st circulation candidate refers 901, 902 is referred to by the 2nd circulation candidate, and 903 is referred to by the 3rd circulation candidate. 904-906 are the data enciphered with one encryption key, respectively, The data enciphered with the encryption key in which the 1st circulation candidate (for example, manager) has 904, the data enciphered with the encryption key in which the 2nd circulation candidate (for example, section chief) has 905, and 906 are the data enciphered with the encryption key which the 3rd circulation candidate (for example, chief) has. Although the structure of the code data for 3 persons was shown here, this is recursively [for the circulation candidate of the arbitrary numbers] extensible.

[0035]Drawing 13 is the flow chart which showed the flow of processing of this embodiment. Hereafter, operation is explained according to this flow chart. First, the donor of circulating data creates the encryption key for a circulation candidate's number by the computer 806, and makes the auxiliary storage unit 808 memorize (Step 1001). Next, it transmits one encryption key at a time to each user's computers 801-804, respectively (Step 1002).

[0036]Next, a data donor creates the data made to refer to it to each circulation candidate, and inputs into the computer 805 from the input device 807 (Step 1003). Here, each data may differ according to a circulation candidate, and may be the same. It is good also as a piece data group which comprises two or more piece data in the data which one circulation candidate refers to. A meaning respectively ID number is assigned to each data (piece data) created here, and a piece data group is registered into the same table as drawing 3 (Step 1004).

[0037]Hereafter, each piece data group is enciphered in order based on the information on this table. Encryption processing is performed by the computer 806. First, the data 903 referred to at the end is enciphered with the encryption key which the circulation candidate who refers to it at the end has (Step 1005). The data enciphered by this is 906 of drawing 12. Next, it combines with the data which the circulation candidate who refers to circulating data in public [of this circulation candidate / 1] refers to, and said code data 906 (Step 1006). This merge data is enciphered with the enciphering key which the circulation candidate who refers to circulating data has in public [1] (Step 1007). The data enciphered by this is 905 of drawing 12.

[0038]The above operation is repeatedly performed until it enciphers all the piece data groups (Step 1008). Turn of each encryption processing is performed by a circulation candidate's order of circulation and reverse order. The code data which encryption processing finished is memorized by the auxiliary storage unit 809 with the contents of the same piece data group table as drawing 3 (Step 1009).

[0039]Hereafter, decoding and reference are performed in order by the circulation candidate. First, the code data 904 is transmitted to the computer 802 (A) by the circulation candidate of the 1st reference authority ranking via the network 801 from the shared auxiliary storage unit 809. Code data is decrypted with the encryption key distributed to the 1st circulation

candidate (for example, manager) by the computer (A) 802 (Step 1010). Next, according to the same piece data group table as drawing 3, the decrypted piece data 901 is reconstructed like Embodiment 1 (Step 1011). It confirms whether be the format in which the output of the reconstructed data is possible here, and if it is the format in which an output is impossible, the circulation candidate who performed this reference process will judge that he is not the circulation candidate who followed in order of the right, and will interrupt a reference process (Step 1012).

[0040]On the contrary, if it is the format in which an output is possible, it will output in the form where the utilizing method of data was balanced (Step 1013). Here, when the data which the code data 905, i.e., the circulation candidate of the following turn, refers to is contained in the decrypted data, only the code data portion is taken out and it memorizes to the share auxiliary storage unit 809 (Step 1015). The processing for which each circulation candidate refers to the piece data group which he can refer to by decoding code data with the encryption key which he has hereafter is repeated. Processing is ended, when it decrypts and code data is not contained in it.

[0041]Since it is locked by the manager's encryption key, it becomes impossible therefore, to decode circulating data, even if a section chief is going to decode circulating data with the encryption key assigned to itself ahead of the manager in the system which makes a turn system maintain and refer to it in order of the manager, a section chief, and a chief. By this, the turn system which refers to circulating data is certainly maintainable.

[0042]Thus, in this embodiment, data is relayed among two or more data users, When permitting reference of piece data in order, decryption and the reference process of reference part data applicable by the 2nd user only after decryption and the reference process of reference part data applicable by the 1st data user are performed become possible.

[0043]Therefore, offer of the encryption key for corresponding decoding to the 2nd data user from a data donor, It becomes possible not to be because decryption and the reference process of the 1st data user's reference part data to be executed, but to carry out, Since it becomes unnecessary to check execution of decryption and the reference process the 1st data user's reference part data by the data donor side, the turn of the reference process of the 1st data user and the 2nd data user can be checked easily.

[0044]

[Effect of the Invention]The inside of the circulating data set which comprises fundamentally two or more piece data provided by the circulating data donor side device as mentioned above according to this invention, On condition that all the users who have the reference authority ranking of a higher rank rather than the user concerned are ending with reference, in order to enable the reference of the specific piece data of the reference authority ranking which the user of the circulating data user side device demands, The encryption key of the number of reference authority ranking and the same number which were set up to the circulating data set which comprises two or more piece data in the circulating data donor side device is generated or set up, As opposed to the specific piece data corresponding to [transmit to the circulating data user side device, and] one reference authority ranking, The encryption partial data set which enciphered all the piece data referred to by the user of the reference authority after the following ranking with the encryption key corresponding to the reference authority ranking is added, The processing which enciphers the data set which comprises these specific piece data and an encryption partial data set with the encryption key corresponding to the reference authority ranking concerned, The number of reference authority ranking and the number-of-times line of said acquire the circulating data set which enciphered the whole data set, stored this enciphered circulating data set in memory storage, and was stored in said memory storage in the circulating data user side device according to the demand from a circulating data user, Decode piece data corresponding with the encryption key corresponding to the reference authority ranking of the user concerned, and output in the form which a data user can refer to, and. Since the encryption piece data concerned was re-stored in said memory storage when encryption piece data existed in decoded piece data, When circulating data is relayed among two or more circulating data users and reference of circulating data is permitted in order, Only on the conditions on which decryption and the reference process of circulating data applicable by the data user of the reference authority ranking of a higher rank were performed, decryption and the reference process of circulating data applicable by the user of the reference authority of the following ranking become possible. Therefore, the reference reference of circulating data can be enabled in the turn according to the circulating data user's reference authority ranking, without making complicated processing by the side of a circulating data donor.

[Translation done.]

DESCRIPTION OF DRAWINGS

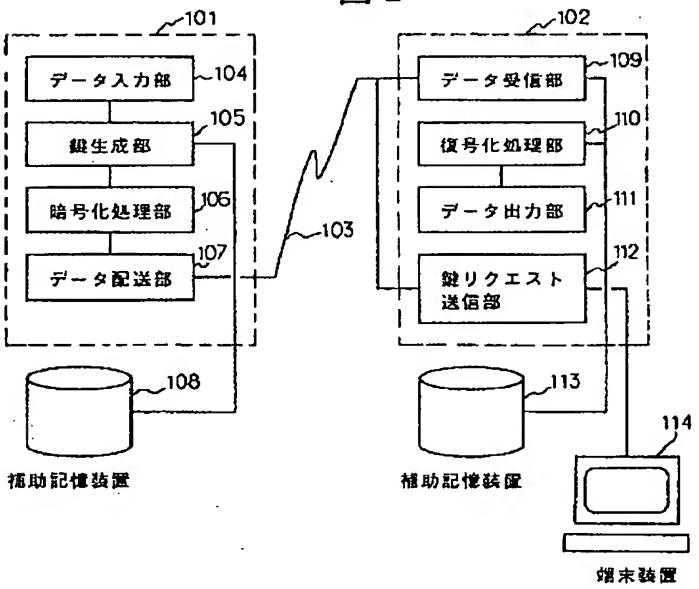
[Brief Description of the Drawings]
[Drawing 1]It is a block lineblock diagram showing a 1st embodiment of this invention.
[Drawing 2]It is a lineblock diagram of the registration table of piece data.
[Drawing 3]It is a lineblock diagram of the registration table of a piece data group.
[Drawing 4]It is a lineblock diagram of the registration table of an encryption key.
[Drawing 5]It is a lineblock diagram of the unit price table of a piece data group.
[Drawing 6]It is a lineblock diagram of the charge amount registration table of a piece data group.
[Drawing 7]It is a flow chart which shows the data reference process procedure of a 1st embodiment.
[Drawing 8]It is a flow chart which shows a continuation of drawing 7.
[Drawing 9]It is a lineblock diagram showing the example of the code data used by a 1st embodiment.
[Drawing 10]It is a lineblock diagram of the decode data according to reference stage in a 1st embodiment.
[Drawing 11]It is a system configuration figure showing a 2nd embodiment of this invention.
[Drawing 12]It is a lineblock diagram of the code data used by a 2nd embodiment.
[Drawing 13]It is a flow chart which shows the data reference process procedure in a 2nd embodiment.
[Description of Notations]
101,102 -- A computer system, 103 -- A network, 104 -- Data input part, 105 [-- An auxiliary storage unit, 109 / -- A data receiving section, 110 / -- A decoding processing part, 111 / -- A data output part, 112 / -- A key request transmission part, 114 / -- Terminal unit.] -- A key generation part, 106 -- An enciphering processing part, 107 -- A data delivery part, 108,113

[Translation done.]

DRAWINGS

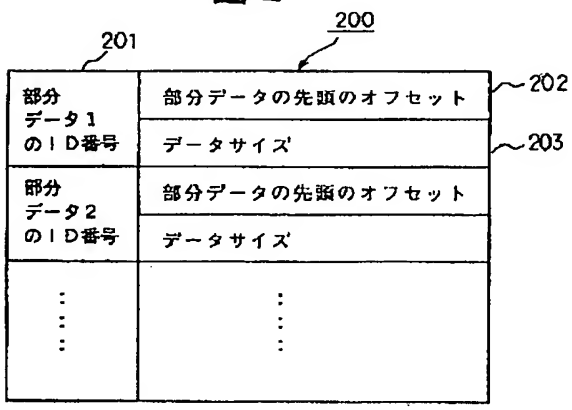
[Drawing 1]

図 1



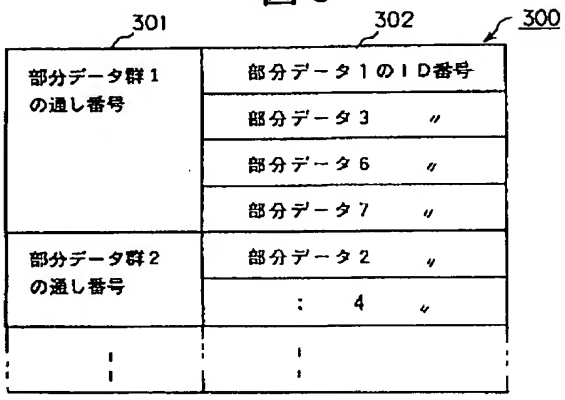
[Drawing 2]

図 2



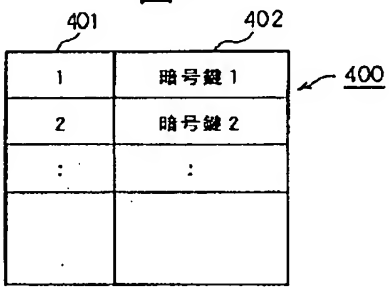
[Drawing 3]

図 3



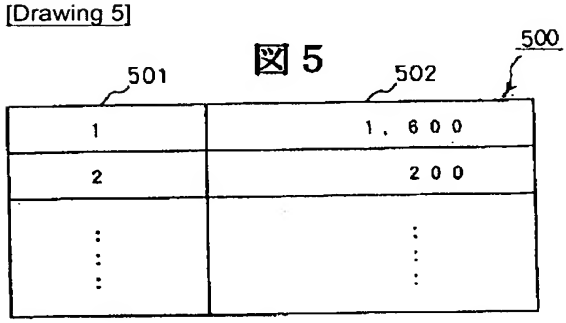
[Drawing 4]

図 4



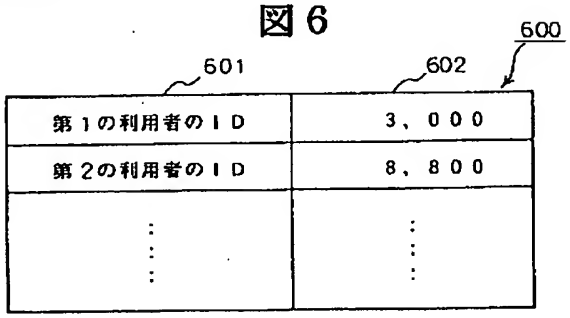
[Drawing 5]

図 5



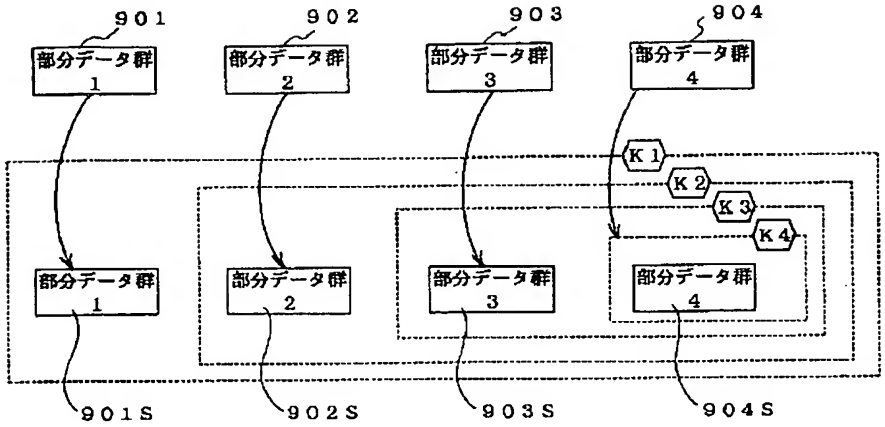
[Drawing 6]

図 6



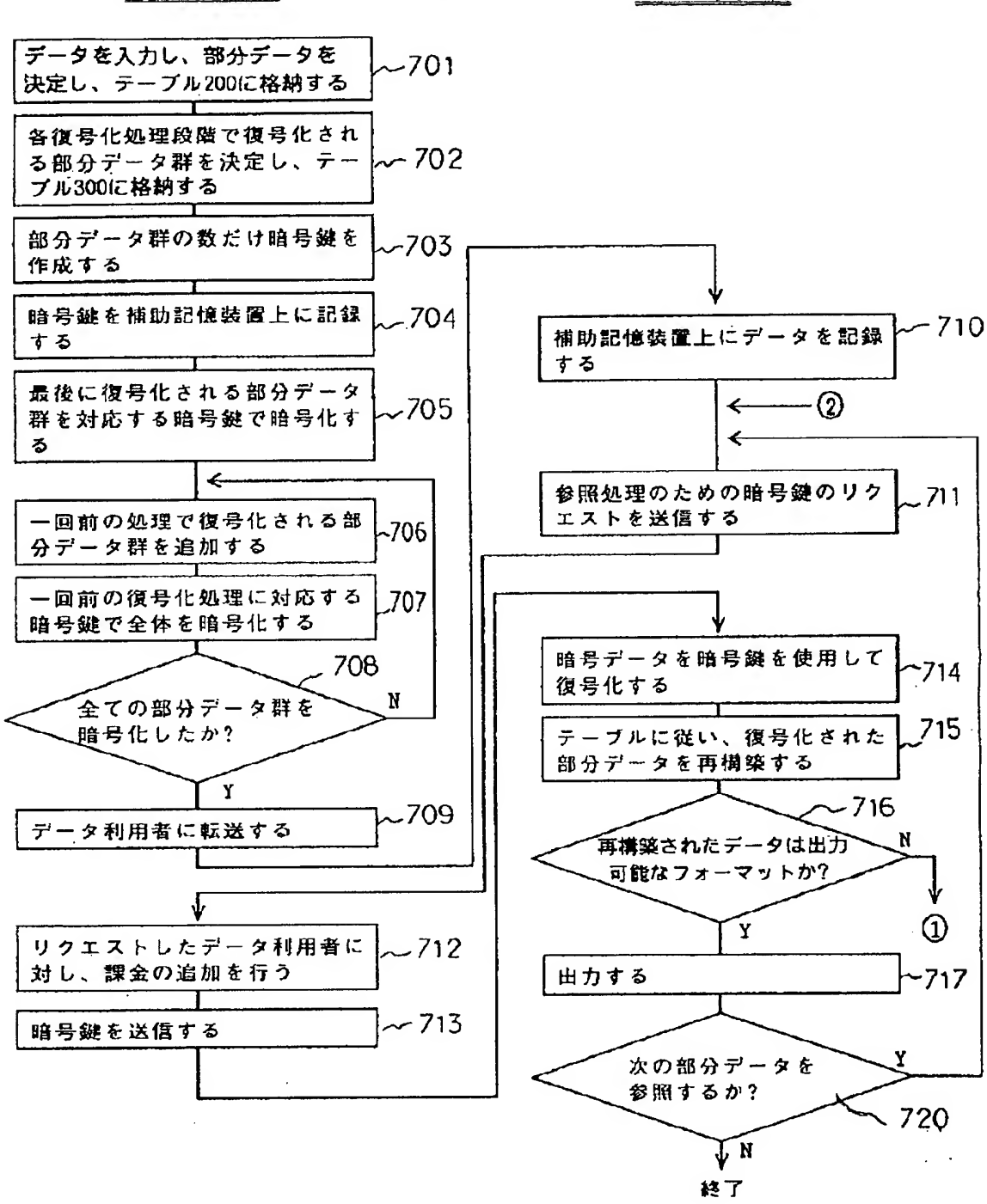
[Drawing 9]

図９


901
902
903
904
部分データ群 1
部分データ群 2
部分データ群 3
部分データ群 4
K 1
K 2
K 3
K 4
部分データ群 1
部分データ群 2
部分データ群 3
部分データ群 4
901S
902S
903S
904S

[Drawing 7]

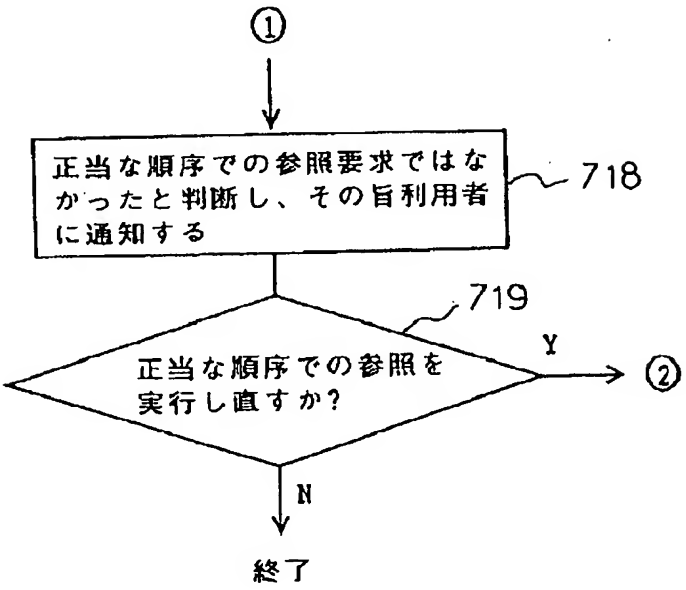
図 7


データ提供者側
データ利用者側
データを入力し、部分データを決定し、テーブル200に格納する
701
各復号化処理段階で復号化される部分データ群を決定し、テーブル300に格納する
702
部分データ群の数だけ暗号鍵を作成する
703
暗号鍵を補助記憶装置上に記録する
704
最後に復号化される部分データ群を対応する暗号鍵で暗号化する
705
一回前の処理で復号化される部分データ群を追加する
706
一回前の復号化処理に対応する暗号鍵で全体を暗号化する
707
全ての部分データ群を暗号化したか?
708
N
Y
データ利用者に転送する
709
リクエストしたデータ利用者に対し、課金の追加を行う
712
暗号鍵を送信する
713
補助記憶装置上にデータを記録する
710
②
参照処理のための暗号鍵のリクエストを送信する
711
暗号データを暗号鍵を使用して復号化する
714
テーブルに従い、復号化された部分データを再構築する
715
再構築されたデータは出力可能なフォーマットか?
716
N
①
Y
出力する
717
次の部分データを参照するか?
720
Y
N
終了

[Drawing 8]

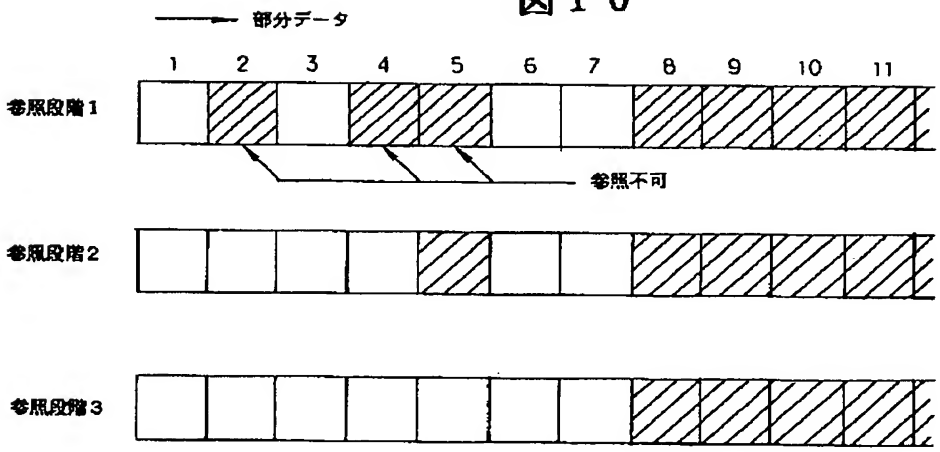
図 8

データ利用者側



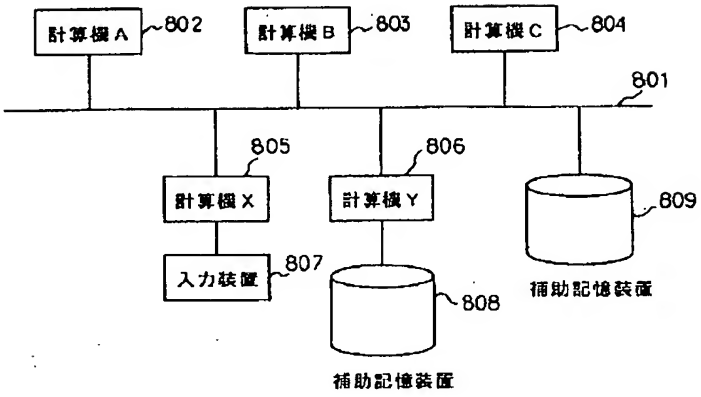
[Drawing 10]

図 1 0



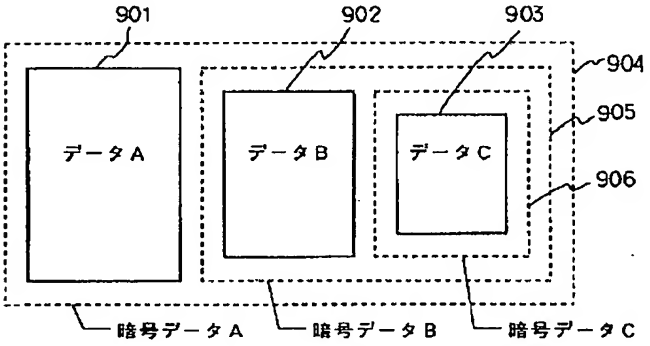
[Drawing 11]

図１１



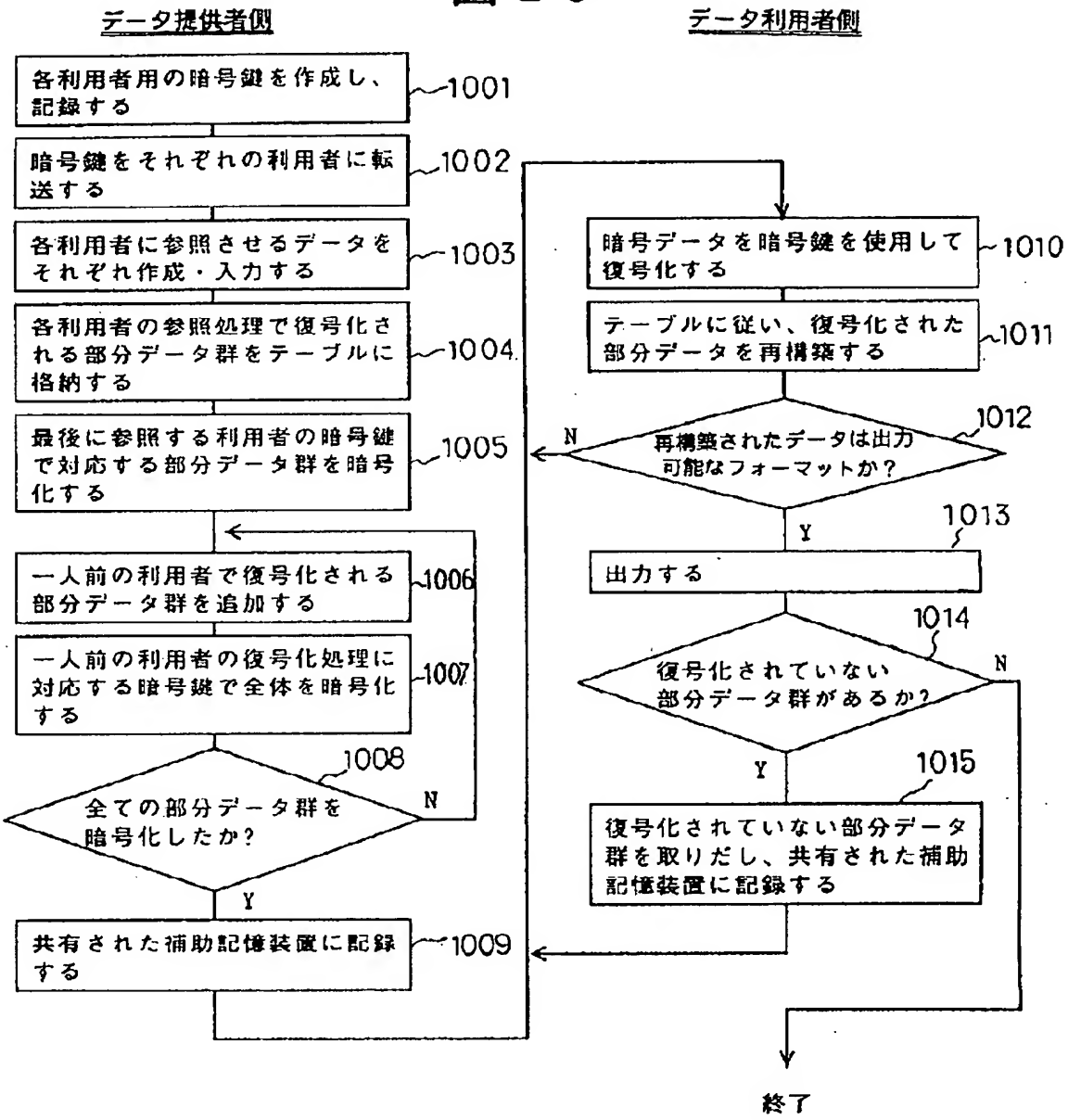
[Drawing 12]

図１２



[Drawing 13]

図１３



[Translation done.]

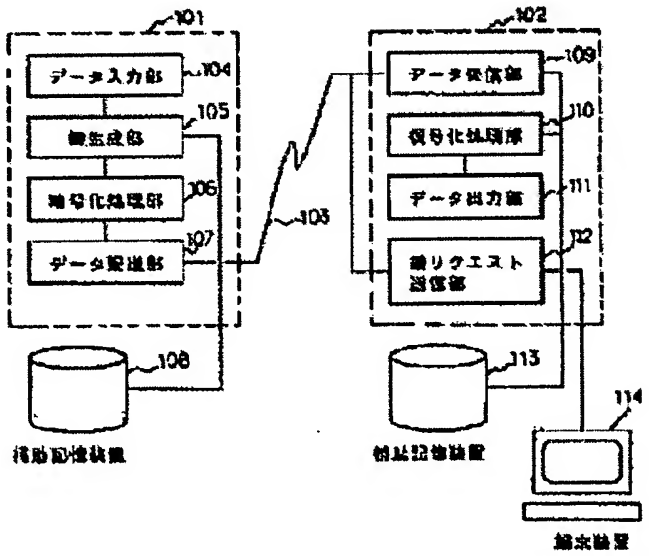
METHOD AND SYSTEM FOR CONTROLLING CIRCULATION DATA REFERENCE ORDER

Publication number: JP2000138667
Publication date: 2000-05-16
Inventor: TAGO SHIGERU
Applicant: HITACHI SOFTWARE ENG
Classification:
- International: ***G06F12/14; G06F21/24; G09C1/00; H04L9/14;*** **G06F12/14; G06F21/00; G09C1/00; H04L9/14;** (IPC1-7): H04L9/14; G06F12/14; G09C1/00
- European:
Application number: JP19990338145 19991129
Priority number(s): JP19990338145 19991129

Report a data error here

Abstract of **JP2000138667**

PROBLEM TO BE SOLVED: To reference circulation data in the order in response to the reference order of data users without making processing by a circulation data server complicated. SOLUTION: A circulation data server side device 101 generates cryptographic keys whose number is the same number as a reference right order number set to a circulation data set consisting of plurality of partial data, transfers the data to the device of a circulation data user, which adds an encrypted partial data set resulting from encrypting all partial data that are referenced by users with next and succeeding ranking reference right by cryptographic key corresponding to the reference right order to specific partial data corresponding to one reference right order, and conducts the processing encrypting a data set consisting of the specific partial data and the encrypted partial data set by using the cryptographic key corresponding to the reference right order for the same number of times as the reference right order number, a user side device 102 acquires the encrypted circulation data set in response to a request from the user, demodulates the corresponding partial data by using the cryptographic key corresponding to the reference right order of the user and provides an output of the decoded data in a form that can be referenced by the data users.



(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号
特開2000－138667
（P2000－138667A）
(43)公開日　平成12年５月16日(2000.5.16)

(51)Int.Cl.⁷	識別記号	ＦＩ		ﾃｰﾏｺｰﾄﾞ(参考)
Ｈ０４Ｌ　9/14		Ｈ０４Ｌ　9/00	６４１	
Ｇ０６Ｆ　12/14	３２０	Ｇ０６Ｆ　12/14	３２０Ｂ	
Ｇ０９Ｃ　1/00	６６０	Ｇ０９Ｃ　1/00	６６０Ｄ	

審査請求　未請求　請求項の数４　ＯＬ　（全 13 頁）

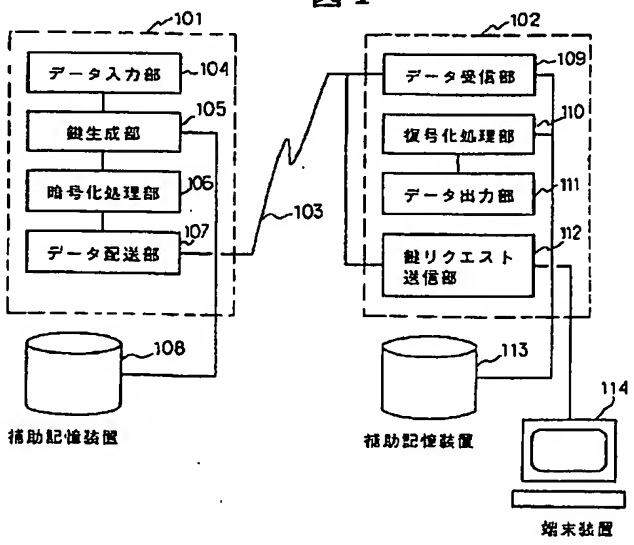
(21)出願番号　特願平11－338145
(62)分割の表示　特願平6－16551の分割
(22)出願日　平成６年２月10日(1994.2.10)

(71)出願人　000233055
日立ソフトウエアエンジニアリング株式会社
神奈川県横浜市中区尾上町６丁目81番地
(72)発明者　多胡　滋
神奈川県横浜市中区尾上町６丁目81番地
日立ソフトウエアエンジニアリング株式会社内
(74)代理人　100083552
弁理士　秋田　収喜

(54)【発明の名称】　回覧データ参照順の制御方法およびシステム

(57)【要約】
【課題】　回覧データ提供者側の処理を煩雑にすることなく、データ利用者の参照順位に応じた順番で回覧データの参照を可能にすること。
【解決手段】　回覧データ提供者側装置において複数の部分データから成る回覧データ集合に対して設定された参照権限順位数と同数の暗号鍵を生成し、回覧データ利用者側装置に転送しておき、１つの参照権限順位に対応した特定の部分データに対し、次順位以降の参照権限の利用者で参照する全ての部分データをその参照権限順位に対応する暗号鍵で暗号化した暗号化部分データ集合を追加し、これら特定の部分データと暗号化部分データ集合とから成るデータ集合を当該参照権限順位に対応した暗号鍵で暗号化する処理を、参照権限順位数と同回数行ってデータ集合全体を暗号化し、この暗号化された回覧データ集合を利用者側装置において利用者からの要求に応じて取得させ、当該利用者の参照権限順位に対応した暗号鍵によって対応する部分データを復号し、データ利用者が参照可能な形式で出力する。

図１



1

【特許請求の範囲】

【請求項１】　回覧データ提供者側装置により提供される複数の部分データから成る回覧データ集合のうち、回覧データ利用者側装置の利用者が要求する参照権限順位の特定の部分データを当該利用者よりも上位の参照権限順位を有する全ての利用者が参照済みであることを条件に参照可能にする回覧データ参照順の制御方法であって、

回覧データ提供者側装置において複数の部分データから成る回覧データ集合に対して設定された参照権限順位数と同数の暗号鍵を生成または設定し、回覧データ利用者側装置に転送するステップと、

１つの参照権限順位に対応した特定の部分データに対し、次順位以降の参照権限の利用者で参照する全ての部分データをその参照権限順位に対応する暗号鍵で暗号化した暗号化部分データ集合を追加し、これら特定の部分データと暗号化部分データ集合とから成るデータ集合を当該参照権限順位に対応した暗号鍵で暗号化する処理を、参照権限順位数と同回数行ってデータ集合全体を暗号化し、この暗号化された回覧データ集合を記憶装置に格納するステップと、

回覧データ利用者側装置において、前記記憶装置に格納された回覧データ集合を回覧データ利用者からの要求に応じて取得し、当該利用者の参照権限順位に対応した暗号鍵によって対応する部分データを復号し、データ利用者が参照可能な形式で出力すると共に、復号した部分データ中に暗号化部分データが存在する場合には当該暗号化部分データを前記記憶装置に再格納するステップと、

を備えることを特徴とする回覧データ参照順の制御方法。

【請求項２】　回覧データ提供者側装置により提供される複数の部分データから成る回覧データ集合のうち、回覧データ利用者側装置の利用者が要求する参照権限順位の特定の部分データを当該利用者よりも上位の参照権限順位を有する全ての利用者が参照済みであることを条件に参照可能にする回覧データ参照順制御システムであって、

前記回覧データ提供者側装置は、複数の部分データから成る回覧データ集合に対して設定された参照権限順位数と同数の暗号鍵を生成または設定し、回覧データ利用者側装置に転送する暗号鍵生成手段と、

１つの参照権限順位に対応した特定の部分データに対し、次順位以降の参照権限の利用者で参照する全ての部分データをその参照権限順位に対応する暗号鍵で暗号化した暗号化部分データ集合を追加し、これら特定の部分データと暗号化部分データ集合とから成るデータ集合を当該参照権限順位に対応した暗号鍵で暗号化する処理を、参照権限順位数と同回数行ってデータ集合全体を暗号化し、この暗号化された回覧データ集合を記憶装置に格納する暗号化処理手段とを具備し、

2

前記回覧データ利用者側装置は、前記記憶装置に格納された回覧データ集合を回覧データ利用者からの要求に応じて取得し、当該利用者の参照権限順位に対応した暗号鍵によって対応する部分データを復号し、データ利用者が参照可能な形式で出力すると共に、復号した部分データ中に暗号化部分データが存在する場合には当該暗号化部分データを前記記憶装置に再格納する復号化処理手段を具備することを特徴とする回覧データ参照順制御システム。

【請求項３】　回覧データ提供者側装置により提供される複数の部分データから成る回覧データ集合のうち、回覧データ利用者側装置の利用者が要求する参照権限順位の特定の部分データを当該利用者よりも上位の参照権限順位を有する全ての利用者が参照済みであることを条件に参照可能にする回覧データ参照順の制御方法であって、

回覧データ提供者側装置において複数の部分データから成る回覧データ集合に対して設定された参照権限順位数と同数の暗号鍵を生成または設定し、回覧データ利用者側装置に転送するステップと、

最下位の参照権限順位に対応した特定の部分データを当該参照権限順位に対応する暗号鍵で暗号化し、該暗号化部分データに対し、１つ上位の参照権限順位の利用者が参照可能な部分データを追加し、これらの暗号化部分データと１つ上位の参照権限順位の部分データとを１つ上位の参照権限順位に対応する暗号鍵で暗号化する処理を、最上位の参照権限順位での部分データの暗号化が終了するまで繰返し、暗号化された回覧データ集合を記憶装置に格納するステップと、

前記回覧データ利用者側装置において、前記記憶装置に格納された回覧データ集合を回覧データ利用者からの要求に応じて取得し、当該利用者の参照権限順位に対応した暗号鍵によって対応する部分データを復号し、データ利用者が参照可能な形式で出力すると共に、復号した部分データ中に暗号化部分データが存在する場合には当該暗号化部分データを前記記憶装置に再格納するステップと、を備えることを特徴とする回覧データ参照順の制御方法。

【請求項４】　回覧データ提供者側装置により提供される複数の部分データから成る回覧データ集合のうち、回覧データ利用者側装置の利用者が要求する参照権限順位の特定の部分データを当該利用者よりも上位の参照権限順位を有する全ての利用者が参照済みであることを条件に参照可能にする回覧データ参照順制御システムであって、

前記回覧データ提供者側装置は、複数の部分データから成る回覧データ集合に対して設定された参照権限順位数と同数の暗号鍵を生成または設定し、回覧データ利用者側装置に転送する暗号鍵生成手段と、

最下位の参照権限順位に対応した特定の部分データを当

該参照権限順位に対応する暗号鍵で暗号化し、該暗号化部分データに対し、１つ上位の参照権限順位の利用者が参照可能な部分データを追加し、これらの暗号化部分データと１つ上位の参照権限順位の部分データとを１つ上位の参照権限順位に対応する暗号鍵で暗号化する処理を、最上位の参照権限順位での部分データの暗号化が終了するまで繰返し、暗号化された回覧データ集合を記憶装置に格納する暗号化処理手段とを具備し、

前記回覧データ利用者側装置は、前記記憶装置に格納された回覧データ集合を回覧データ利用者からの要求に応じて取得し、当該利用者の参照権限順位に対応した暗号鍵によって対応する部分データを復号し、データ利用者が参照可能な形式で出力すると共に、復号した部分データ中に暗号化部分データが存在する場合には当該暗号化部分データを前記記憶装置に再格納する復号化処理処理手段を具備することを特徴とする回覧データ参照順制御システム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、回覧データ提供者により提供される回覧データ集合を回覧データ利用者側で参照するシステムにおける回覧データの参照順の制御方法およびシステムに係り、特に、回覧データの利用者が要求する参照権限順位の特定の部分データを当該利用者よりも上位の参照権限順位を有する全ての利用者が参照済みであることを条件に参照可能にする回覧データ参照順の制御方法及びシステムに関する。

【０００２】

【従来の技術】あるデータを提供者からデータ利用者に提供し、逐次参照させるシステムにおいて、データ提供者側の要求により、そのデータを複数の部分データに分割し、データ利用者がデータを参照する処理を行う段階に応じて、複数ある部分データのうち参照可能なものを限定したい場合がある。例えば、契約上ある時点までは全データのうち特定の部分だけを参照することをデータ利用者に許し、その時点を過ぎれば全データの参照を許す、という場合がある。また、ある有料データを自由に配布した時、各データ利用者ごとに参照したいデータの範囲が異なったり、ある範囲まで参照した上でさらに詳しい範囲のデータを参照したくなったりした際に、利用するデータをより詳しいデータにするために追加課金をするが、この追加分だけの課金でより詳しいデータを利用してしまうことを防ぎたい、という場合がある。あるいは、最初にデータの提供を受けた第１のデータ利用者には全データのうち特定の部分だけを参照することを許し、その全データを次の第２のデータ利用者に中継し、第２のデータ利用者には全データの参照を許す、という場合がある。

【０００３】このようなことを実現するため、従来、以下の技術がある。

（１）全データを１回の手続きでデータ利用者に提供せず、データ利用者の要求に応じて、参照可能とする部分データを順次提供していく。

（２）データを複数の部分データに分割し、それぞれを異なる暗号鍵で暗号化しデータ利用者に提供する。以降、データ利用者の要求に応じて、参照可能とする部分データの復号鍵を順次提供していく。

【０００４】

【発明が解決しようとする課題】しかし、これらの方法では次のような問題がある。

（１）ある部分データをデータ提供者からデータ利用者に提供する段階で、その部分データを参照可能にする条件として、別の部分データをデータ利用者が参照済みであることを要求されている場合、データ利用者がこの条件を満たしているかどうかをデータ提供者側で管理した上で、対象となる部分データを提供するかどうかを判断する必要がある。そのためには、各部分データを過去にデータ利用者に提供したかどうか、あるいは、データ利用者によって各部分データの参照処理が実行されたかどうかといった情報を全データ利用者および全部分データに関して入手あるいは保持し、管理する必要がある。この結果、データ提供者側の処理が非常に煩雑になる。

【０００５】（２）特に、複数のデータ利用者によって異なる部分データの参照を許可する場合、あるデータ利用者（第１のデータ利用者）が該当する部分データを参照した後に、別のデータ利用者（第２のデータ利用者）が該当する部分データを参照することが可能になるという要求のもとでは、データ提供者側で、第１のデータ利用者が該当する部分データを参照したことを確認した上で、第２のデータ利用者に対し部分データの提供あるいは対応する復号鍵の提供を実行しなければならず、データ提供者側の処理が非常に煩雑になる。

【０００６】本発明の目的は、データ提供者側の処理を煩雑にすることなく、回覧データの利用者が要求する参照権限順位の特定の部分データを当該利用者よりも上位の参照権限順位を有する全ての利用者が参照済みであることを条件に参照可能にする回覧データ参照順の制御方法およびシステムを提供することである。

【０００７】

【課題を解決するための手段】上記目的を達成するために、本発明は、基本的には、回覧データの利用者が要求する参照権限順位の特定の部分データを当該利用者よりも上位の参照権限順位を有する全ての利用者が参照済みであることを条件に参照可能にするために、回覧データ提供者側装置において複数の部分データから成る回覧データ集合に対して設定された参照権限順位数と同数の暗号鍵を生成または設定し、回覧データ利用者側装置に転送するステップと、１つの参照権限順位に対応した特定の部分データに対し、次順位以降の参照権限の利用者で参照する全ての部分データをその参照権限順位に対応す

る暗号鍵で暗号化した暗号化部分データ集合を追加し、これら特定の部分データと暗号化部分データ集合とから成るデータ集合を当該参照権限順位に対応した暗号鍵で暗号化する処理を、参照権限順位数と同回数行ってデータ集合全体を暗号化し、この暗号化された回覧データ集合を記憶装置に格納するステップと、回覧データ利用者側装置において、前記記憶装置に格納された回覧データ集合を回覧データ利用者からの要求に応じて取得し、当該利用者の参照権限順位に対応した暗号鍵によって対応する部分データを復号し、データ利用者が参照可能な形式で出力すると共に、復号した部分データ中に暗号化部分データが存在する場合には当該暗号化部分データを前記記憶装置に再格納するステップとを備えることを特徴とする。

【０００８】上記手段によれば、複数のデータ利用者間でデータを中継し、順番に部分データの参照を許可するような回覧システムにおいて、最上位の参照権限順位を有する第１のデータ利用者によって該当する参照部分データの復号化・参照処理が実行されて初めて次の順位の第２の利用者によって該当する参照部分データの復号化・参照処理が可能になる。すなわち、回覧データ提供者側から提供される回覧データのうち、データ利用者がある自分への回覧データを参照したい場合、自分の参照権限順位よりも上位の参照権限順位を有する全ての利用者が参照すべき回覧データを参照していることが条件となり、この条件が満たされている場合にのみ自分が参照権限を有する回覧データを参照することができ、参照権限順に、回覧データを参照することを保証することができる。

【０００９】従って、回覧データ提供者から第２のデータ利用者への対応する復号のための暗号鍵の提供は、最上位の参照権限順位を有する第１のデータ利用者の参照部分データの復号化・参照処理が実行済みであるか否かによらず行うことが可能になり、第１のデータ利用者の参照部分データの復号化・参照処理の実行をデータ提供者側で確認することが不要となるため、第１のデータ利用者と第２のデータ利用者の参照処理の順番を簡単に確認することができる。

【００１０】

【発明の実施の形態】以下、本発明の実施の形態を図面に従い説明する。

（実施形態１）データ提供者によってデータを広範囲に不特定多数のデータ利用者に配布し、データ利用者の希望によって、配布されたデータのうち参照可能となるデータの範囲を狭いものから広いものに変更し、その際に狭い参照データ範囲に対する課金内容に対して上乗せする形で追加課金するデータ多段階参照システムの実施形態を説明する。このシステムは、例えば、ゲームソフトの配布システムとして、まず利用者にゲームソフトの一部の機能や画面データだけを試用してもらい、引き続いてゲーム全体を楽しみたいという意志が利用者にあれば、それに対する追加料金を払ってもらうことで、ゲーム全体の使用を許すという場合に適用されるものである。

【００１１】図１は、このようなシステムの一実施形態を示すシステム構成図である。図１において、１０１はデータ提供者側の計算機システム、１０２はデータ利用者側の計算機システム、１０３は計算機システム１０１と１０２とを接続し、データを転送するネットワーク、１０４はデータ提供者側から提供するデータを入力するデータ入力部である。このデータ入力部１０４は、キーボード、マウス、マイクロフォン、ビデオ撮影機などで構成される。１０５は暗号鍵生成部、１０６は暗号鍵生成部１０５によって生成された暗号鍵を利用してデータの暗号化を行う暗号化処理部、１０７は暗号化処理部１０６で暗号化されたデータをネットワーク１０３を介して利用者側の計算機システム１０２に転送する処理を行うデータ配送部、１０８は鍵生成部１０５で生成された鍵グループを記憶しておく補助記憶装置である。１０９はネットワーク１０３を介して転送されてきたデータを受信するデータ受信部、１１０は暗号データを暗号鍵によって復号化する処理を行う復号化処理部、１１１は復号化処理部１１０で復号化されたデータを出力するデータ出力部であり、このデータ出力部１１は例えばディスプレイ、スピーカ、印字装置等で構成される。

【００１２】１１２はデータ提供者に対し、暗号データの復号に用いる暗号鍵を転送するように要求する鍵リクエストをネットワーク１０３を介して送信する鍵リクエスト送信部（暗号鍵取得手段）、１１３はデータ提供者から配布されたデータを記憶しておく補助記憶装置、１１４はデータ利用者が鍵リクエストを送信するための命令を入力する端末装置である。

【００１３】図２は、データ提供者が提供するデータ全体を複数の部分データに分割した時の各部分データの全データに対する範囲を記録するテーブル２００の構成図であり、部分データ毎に３つの格納エリア２０１，２０２，２０３で構成されている。このうち格納エリア２０１は、分割された各部分データに対して割り当てられたＩＤ番号を格納するエリア、２０２は全データの先頭データから該当部分データの先頭データまでのオフセット値を格納するエリア、２０３は各部分データの大きさ（データサイズ）を格納するエリアである。

【００１４】図３は、本実施形態における課金方法に関連して、異なる課金によって参照可能とする複数の部分データを部分データ群としてまとめた場合の分類を記録するテーブル３００を示し、部分データ群の通し番号を格納するエリア３０１と、該当する部分データ群に含まれる部分データのＩＤ番号を格納するエリア３０２とから成っている。図３の例では、部分データ群１が部分データ１，３，６，７で構成された場合の通し番号と部分

データＩＤ番号との関係を示している。

【００１５】図４は、各部分データ群を暗号化・復号化するのに用いる暗号鍵を格納するテーブル４００を示し、部分データ群の通し番号を格納するエリア４０１と、その通し番号に対応する暗号鍵データを格納するエリア４０２を備えている。

【００１６】図５は、各部分データ群を参照するために追加課金される額を格納するテーブル５００を示し、通し番号５０１で示される部分データ群に対し、それを参照するために追加課金される額を格納するエリア５０２を備えている。

【００１７】図６は、各データ利用者に課金される課金額の累計を格納するテーブル６００を示し、各データ利用者の銀行口座番号や運転免許証のＩＤなどのデータ利用者ＩＤを格納するエリア６０１と、過去においてデータ提供者から入手・参照したデータに対する課金額の累計をデータ利用者別に格納するエリア６０２が設けられている。

【００１８】図７および図８は、本実施形態の処理の流れを示すフローチャートである。以下、このフローチャートに従い、動作を説明する。まず、データ提供者側でデータ入力部１０４から提供データの入力を行い、これを参照のための課金額の違いによって部分データに分割し、分割された部分データの範囲を図２のテーブル２００に格納する（ステップ７０１）。次に、同じ課金額によって参照可能となる部分データをまとめて、部分データ群とし、図３のテーブル３００に格納する（ステップ７０２）。このテーブル３００により、データ利用者は、ある追加料金を支払うことによって該当する部分データ群をすべて参照することができるようになる。

【００１９】ここで、部分データは、その参照順に部分データ１、２，３…，…という具合に通し番号順に並んだものとなっているが、部分データ群としてまとめる時には、今回参照した部分データと次に参照する部分データとが異なる部分データ群に属するようにまとめられる。

【００２０】次に、このようにして作成した部分データ群の数と同数分の暗号鍵を鍵生成部１０５で作成する（ステップ７０３）。この場合、全ての鍵が異なっていることが望ましい。ここで生成された暗号鍵群は、補助記憶装置１０８に記憶される（ステップ７０４）。次に、利用者に提供するデータを暗号化する処理を行う。まず、最終的な課金額が最も大きく最後に復号化されるべき部分データ群を暗号鍵の１つで暗号化し、図４のテーブル４００の部分データ群通し番号格納エリア４０１のうち今回使用した暗号鍵に対応した通し番号格納エリアに、暗号化した部分データ群の通し番号を格納する（ステップ７０５）。

【００２１】次に、この部分データ群を復号化する１つ前の復号化処理で復号化される部分データ群と、ステップ７０５で暗号化したデータとを連結して１組のデータを作成する（ステップ７０６）。ここで作成された組合せデータを、ステップ７０５は別の暗号鍵で暗号化し、図４のテーブル４００の通し番号格納エリア４０１のうち今回使用した暗号鍵に対応した通し番号格納エリアに、暗号化した部分データ群の通し番号を格納する（ステップ７０７）。次に、さらにもう１つ前の復号化処理で復号化される部分データ群と、ステップ７０７で暗号化したデータとを連結して１組のデータを作成する（ステップ７０６）。以降、これを提供データの全部分データ群を暗号化し終わるまで繰り返す（ステップ７０８）。

【００２２】例えば、図９に示すように４つの部分データ群９０１～９０４に提供データが分割されたとすると、最初は、最後に参照可能となる部分データ群９０４が対応する暗号鍵Ｋ４によって暗号化され、次にその暗号化データ９０４Ｓが１段階前に参照される部分データ群９０３に追加され、これら部分データ群９０３と暗号化データ９０４Ｓとが対応する暗号鍵Ｋ３によって暗号化される。

【００２３】次に、同様にして、暗号化データ９０３Ｓが１段階前に参照される部分データ群９０２に追加され、これら部分データ群９０２と暗号化データ９０３Ｓとが対応する暗号鍵Ｋ２によって暗号化される。最後に、暗号化データ９０２Ｓが１段階前に参照される部分データ群９０１に追加され、これら部分データ群９０１と暗号化データ９０２Ｓとが対応する暗号鍵Ｋ２によって暗号化される。

【００２４】このようにして暗号化が終了した提供データは、データ配送部１０７によってネットワーク１０３を介してデータ利用者側の計算機システム１０２に転送される（ステップ７０９）。この時、同時に図２および図３のテーブル２００，３００の内容も転送される。転送の方法は、共有できる補助記憶装置に保存しておいて任意に転送してもらうか、予め転送要求を受付けておいて各利用者に個別に転送する方法などが考えられる。利用者側の計算機システム１０２に転送された暗号化提供データおよびテーブル２００，３００のデータはデータ利用者側の補助記憶装置１１２に記憶される（ステップ７１０）。この時点以降は、データ利用者は参照したい範囲の部分データ群を復号化するための暗号鍵をデータ提供者からその代金と引替えに取得することができるようになる。

【００２５】ここでは、課金額の小さいものを参照後、課金額の大きいものへと参照できるデータの範囲を順次拡大していく例を説明する。なお、一定範囲の複数の部分データ群を始めから参照したい場合は、１回の処理で複数の暗号鍵を取得する方法も同様に実現することができる。

【００２６】まず、最初の部分データ群を参照するため

に、データ利用者は端末装置１１５から鍵リクエスト送信命令を入力し、鍵リクエスト送信部１１４によってネットワーク１０３を介してデータ提供者側に鍵リクエストを送信させる（ステップ７１１）。この際、図３のテーブル３００の内容を参照し、参照希望の部分データ群のＩＤ番号を同時に送信する。鍵リクエストを受信したデータ提供者の計算機システム１０１は、図５のテーブル５００から鍵リクエストを受けた部分データ群の課金額を検索し、その額を図６のテーブル６００の累計額格納エリアのうち鍵リクエストを送信したデータ利用者に対応する累計学格納エリアの現在の累計額に加算する（ステップ７１２）。

【００２７】続いて、リクエストを受けた部分データ群を暗号化した時の暗号鍵のデータをデータ利用者側に送信する（ステップ７１３）。暗号鍵データを受信したデータ利用者側の計算機システム１０２の復号化処理部１１０は、転送されて来た暗号鍵データを用いて参照希望の部分データ群を含む暗号データ全体を復号化する（ステップ７１４）。次に、データ出力部１１１は、部分データ群が複数の部分データから成っているので、異なる部分データ群に属する部分データ同士の順序を図２および図３のテーブル２００，３００の内容を元に再構築する（ステップ７１５）。

【００２８】次に、データ出力部１１１は、再構築されたデータが出力可能なフォーマットであるかどうかのチェックを行い（ステップ７１６）、もし出力可能でない場合は、この参照処理を実行しようとしたデータ利用者は該当する部分データの参照が許されている段階にない、すなわち該当する部分データより以前に参照しておかねばならない部分データに対する正規の参照処理をまだ実行していないと判断し、その旨を端末装置１１４からデータ利用者に通知する（ステップ７１８）。もし、データ利用者が引き続き正当な順序での部分データの参照を行うことによって該当する部分データの参照を希望する場合は、該当する正当な鍵リクエストの送信を実行し直す（ステップ７１９）。不正に該当する部分データを参照しようとした場合などのように、正当な順序の処理をやり直す意志がデータ利用者にない場合は、処理全体を終了する。

【００２９】もしステップ７１６で出力可能なフォーマットであると判断された場合は、再構築されたデータはデータの利用方法に見合った形で出力される（ステップ７１６）。ここで、さらに次の部分データ群を参照する旨の操作が端末装置１１４で行われた場合は、ステップ７２０からステップ７１１に戻り、以上の処理を繰返し行う。これにより、データ提供者が提供するデータ中に用意されている部分データ群を希望する範囲まで段階的に順次参照することができる。

【００３０】すなわち、図３のテーブル３００によれば、最初に参照される部分データ群として、部分データ１，３，６，７が割り当てられており、次の段階に参照される部分データ群として部分データ２，４，…が割り当てられているので、正規の参照段階順番に対応する暗号鍵を取得し、この暗号鍵で提供データを復号した場合、最初の参照段階１では、図１０に白枠で示すように、部分データ１，３，６，７のみが復号されて利用者に参照可能な形式で出力され、次の参照段階２では、部分データ２，４がさらに参照可能な形式で出力される。そして、次の参照段階３では部分データ５がさらに参照可能な形式で出力される。この繰返しによって部分データ群を希望する範囲まで段階的に順次参照することができる。

【００３１】しかし、部分データ群１を最初に参照せず、次の部分データ群２に対応する暗号鍵で提供データを参照しようとした場合、部分データ群１が未だ復号されていないため、部分データ群２を復号することはできない。従って、１段階前の参照処理を不正に省略し、あるいはデータ提供者から１段階前の参照処理に対応する暗号鍵の提供を受けずに、現段階で参照したい部分データを復号化することを防止することが簡単に実現できる。

【００３２】（実施形態２）次に、複数の利用者の間でデータを回覧する際に、その回覧順序を操作するシステムの実施形態について説明する。このようなシステムは、例えば、企業内で取り交わされている文書において、主任よりも課長、課長よりも部長が先に、すなわち参照権限順位が上位の者から順に、その文書を読むように強制する必要がある回覧物がある場合に適用する。

【００３３】図１１は、本実施形態のシステム構成を示すものであり、８０１はデータ転送を行うネットワークである。８０２（Ａ），８０３（Ｂ），８０４（Ｃ），８０５（Ｘ），８１６（Ｙ）は実施形態１に示した計算機システム１０１，１０２と同様の処理を行う計算機である。８０７は回覧するデータを入力する入力装置である。８０８は複数の暗号鍵を記憶しておく補助記憶装置であり、計算機８０６（Ｙ）に接続されている。８０９は暗号データを記憶し、各利用者からアクセスすることが可能な共有された補助記憶装置である。

【００３４】図１２は、本実施形態で回覧される暗号データの構成を示している。９０１～９０３は異なる利用者によってそれぞれ参照される回覧データであり、９０１は１番目の回覧対象者、９０２は２番目の回覧対象者、９０３は３番目の回覧対象者によって参照されるデータである。９０４～９０６はそれぞれ１個の暗号鍵で暗号化されたデータであり、９０４は１番目の回覧対象者（例えば、部長）が持つ暗号鍵で暗号化されたデータ、９０５は２番目の回覧対象者（例えば、課長）が持つ暗号鍵で暗号化されたデータ、９０６は３番目の回覧対象者（例えば、主任）が持つ暗号鍵で暗号化されたデータである。ここでは３人分の暗号データの構造を示し

たが、これを任意の人数の回覧対象者のために再帰的に拡張できる。

【００３５】図１３は、本実施形態の処理の流れを示したフローチャートである。以下、このフローチャートに従い、動作を説明する。まず、回覧データの提供者は、回覧対象者の人数分の暗号鍵を計算機８０６で作成し、補助記憶装置８０８に記憶させる（ステップ１００１）。次に、暗号鍵をそれぞれ１つづつ各利用者の計算機８０１～８０４に転送する（ステップ１００２）。

【００３６】次にデータ提供者は各回覧対象者に参照させるデータを作成し、入力装置８０７から計算機８０５に入力する（ステップ１００３）。ここで、各データは回覧対象者別に異なるものでもよいし、同一のものでもよい。また、１人の回覧対象者が参照するデータを複数の部分データから成る部分データ群としてもよい。ここで作成された各データ（部分データ）にはそれぞれ一意なＩＤ番号を割当て、図３と同様のテーブルに部分データ群の登録を行う（ステップ１００４）。

【００３７】以下、このテーブルの情報を基に、各部分データ群を順番に暗号化していく。暗号化処理は計算機８０６で実行される。まず、最後に参照されるデータ９０３を最後に参照する回覧対象者の持つ暗号鍵で暗号化する（ステップ１００５）。これによって暗号化されたデータが図１２の９０６である。次に、この回覧対象者の１人前に回覧データを参照する回覧対象者が参照するデータと前記暗号データ９０６と組み合わせる（ステップ１００６）。この組合せデータを１人前に回覧データを参照する回覧対象者の持つ暗号化鍵で暗号化する（ステップ１００７）。これによって暗号化されたデータが図１２の９０５である。

【００３８】以上の操作を全ての部分データ群を暗号化するまで繰返し実行する（ステップ１００８）。各暗号化処理の順番は、回覧対象者の回覧順と逆順で行われる。暗号化処理の終わった暗号データは図３と同様の部分データ群テーブルの内容と共に補助記憶装置８０９に記憶される（ステップ１００９）。

【００３９】以下、回覧対象者によって順番に復号・参照が実行される。まず、１番目の参照権限順位の回覧対象者によって、共有された補助記憶装置８０９から暗号データ９０４がネットワーク８０１を介して計算機８０２（Ａ）に転送される。計算機（Ａ）８０２で１番目の回覧対象者（例えば部長）に配布された暗号鍵によって暗号データを復号化する（ステップ１０１０）。次に、図３と同様の部分データ群テーブルに従い、復号化された部分データ９０１を実施形態１と同様に再構築する（ステップ１０１１）。ここで、再構築されたデータが出力可能なフォーマットであるかどうかをチェックし、出力不可能なフォーマットであれば、この参照処理を実行した回覧対象者は正しい順序に従った回覧対象者ではないと判断し、参照処理を中断する（ステップ１０１２）。

【００４０】逆に、出力可能なフォーマットであれば、データの利用方法に見合った形で出力する（ステップ１０１３）。ここで、復号化されたデータの中に暗号データ９０５すなわち次の順番の回覧対象者が参照するデータが含まれている場合は、その暗号データ部分だけを取り出し、共有補助記憶装置８０９に記憶する（ステップ１０１５）。以下、各回覧対象者が自分が持っている暗号鍵で暗号データを復号することで自分が参照可能な部分データ群を参照する処理を繰り返す。復号化した時点でその中に暗号データが含まれていない場合は処理を終了する。

【００４１】従って、回覧データを部長、課長、主任の順に順番制を維持して参照させるシステムにおいては、課長が部長より先に自分自身に割り当てられた暗号鍵によって復号しようとしても、部長の暗号鍵によってロックされているため、回覧データを復号することができなくなる。これによって、回覧データを参照する順番制を確実に維持することができる。

【００４２】このように本実施形態においては、複数のデータ利用者間でデータを中継し、順番に部分データの参照を許可する場合、第１のデータ利用者によって該当する参照部分データの復号化・参照処理が実行されて初めて第２の利用者によって該当する参照部分データの復号化・参照処理が可能になる。

【００４３】従って、データ提供者から第２のデータ利用者への対応する復号のための暗号鍵の提供は、第１のデータ利用者の参照部分データの復号化・参照処理が実行済みであるか否かによらず行うことが可能になり、第１のデータ利用者の参照部分データの復号化・参照処理の実行をデータ提供者側で確認することが不要となるため、第１のデータ利用者と第２のデータ利用者の参照処理の順番を簡単に確認することができる。

【００４４】

【発明の効果】以上のように本発明によれば、基本的には、回覧データ提供者側装置により提供される複数の部分データから成る回覧データ集合のうち、回覧データ利用者側装置の利用者が要求する参照権限順位の特定の部分データを当該利用者よりも上位の参照権限順位を有する全ての利用者が参照済みであることを条件に参照可能にするために、回覧データ提供者側装置において複数の部分データから成る回覧データ集合に対して設定された参照権限順位数と同数の暗号鍵を生成または設定し、回覧データ利用者側装置に転送しておき、１つの参照権限順位に対応した特定の部分データに対し、次順位以降の参照権限の利用者で参照する全ての部分データをその参照権限順位に対応する暗号鍵で暗号化した暗号化部分データ集合を追加し、これら特定の部分データと暗号化部分データ集合とから成るデータ集合を当該参照権限順位に対応した暗号鍵で暗号化する処理を、参照権限順位数

13

と同回数行ってデータ集合全体を暗号化し、この暗号化された回覧データ集合を記憶装置に格納し、回覧データ利用者側装置において、前記記憶装置に格納された回覧データ集合を回覧データ利用者からの要求に応じて取得し、当該利用者の参照権限順位に対応した暗号鍵によって対応する部分データを復号し、データ利用者が参照可能な形式で出力すると共に、復号した部分データ中に暗号化部分データが存在する場合には当該暗号化部分データを前記記憶装置に再格納するようにしたので、複数の回覧データ利用者間で回覧データを中継し、順番に回覧データの参照を許可する場合、上位の参照権限順位のデータ利用者によって該当する回覧データの復号化・参照処理が実行された条件でのみ、次の順位の参照権限の利用者によって該当する回覧データの復号化・参照処理が可能になる。従って、回覧データ提供者側の処理を煩雑にすることなく、回覧データ利用者の参照権限順位に応じた順番で回覧データを参照参照可能にすることができる。

【図面の簡単な説明】

【図１】本発明の第１の実施形態を示すブロック構成図である。

【図２】部分データの登録テーブルの構成図である。

【図３】部分データ群の登録テーブルの構成図である。

【図４】暗号鍵の登録テーブルの構成図である。

14

【図５】部分データ群の単価テーブルの構成図である。

【図６】部分データ群の課金額登録テーブルの構成図である。

【図７】第１の実施形態のデータ参照処理手順を示すフローチャートである。

【図８】図７の続きを示すフローチャートである。

【図９】第１の実施形態で使用する暗号データの例を示す構成図である。

【図１０】第１の実施形態における参照段階別の復号データの構成図である。

【図１１】本発明の第２の実施形態を示すシステム構成図である。

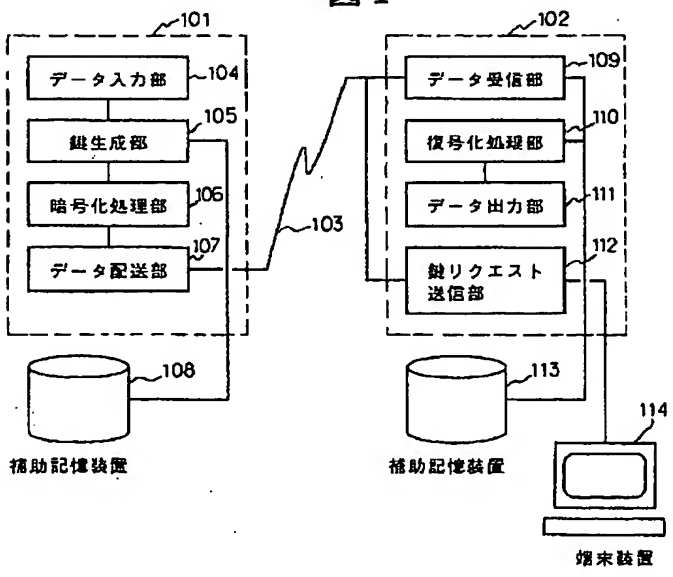
【図１２】第２の実施形態で使用する暗号データの構成図である。

【図１３】第２の実施形態におけるデータ参照処理手順を示すフローチャートである。

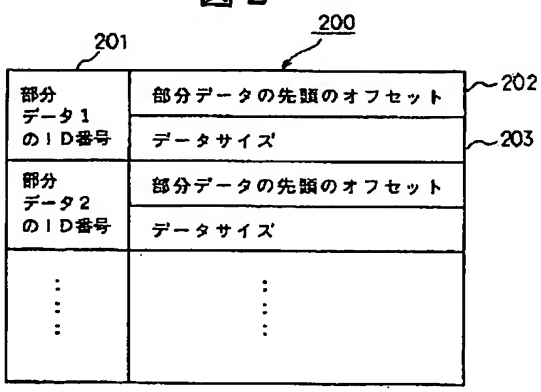
【符号の説明】

１０１，１０２…計算機システム、１０３…ネットワーク、１０４…データ入力部、１０５…鍵生成部、１０６…暗号化処理部、１０７…データ配送部、１０８，１１３…補助記憶装置、１０９…データ受信部、１１０…復号化処理部、１１１…データ出力部、１１２…鍵リクエスト送信部、１１４…端末装置。

【図１】

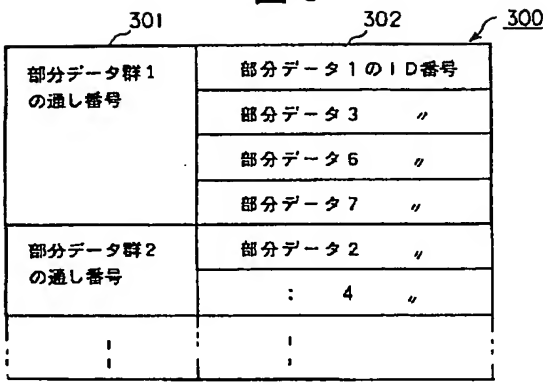


【図２】



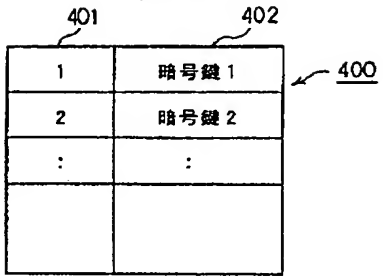
【図３】

図３



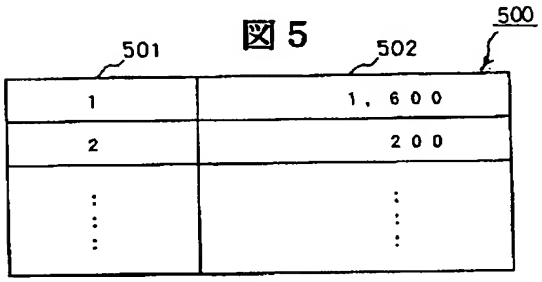
【図４】

図４



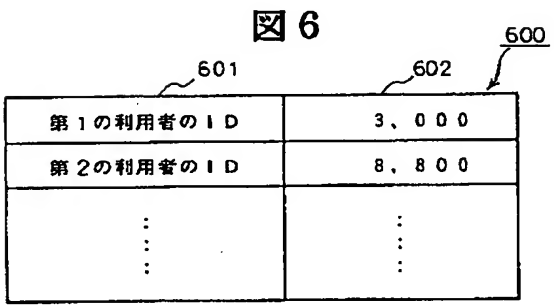
【図５】

図５



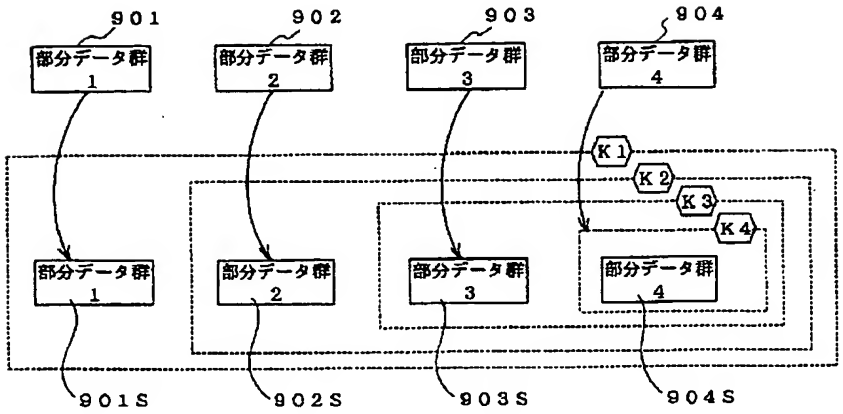
【図６】

図６



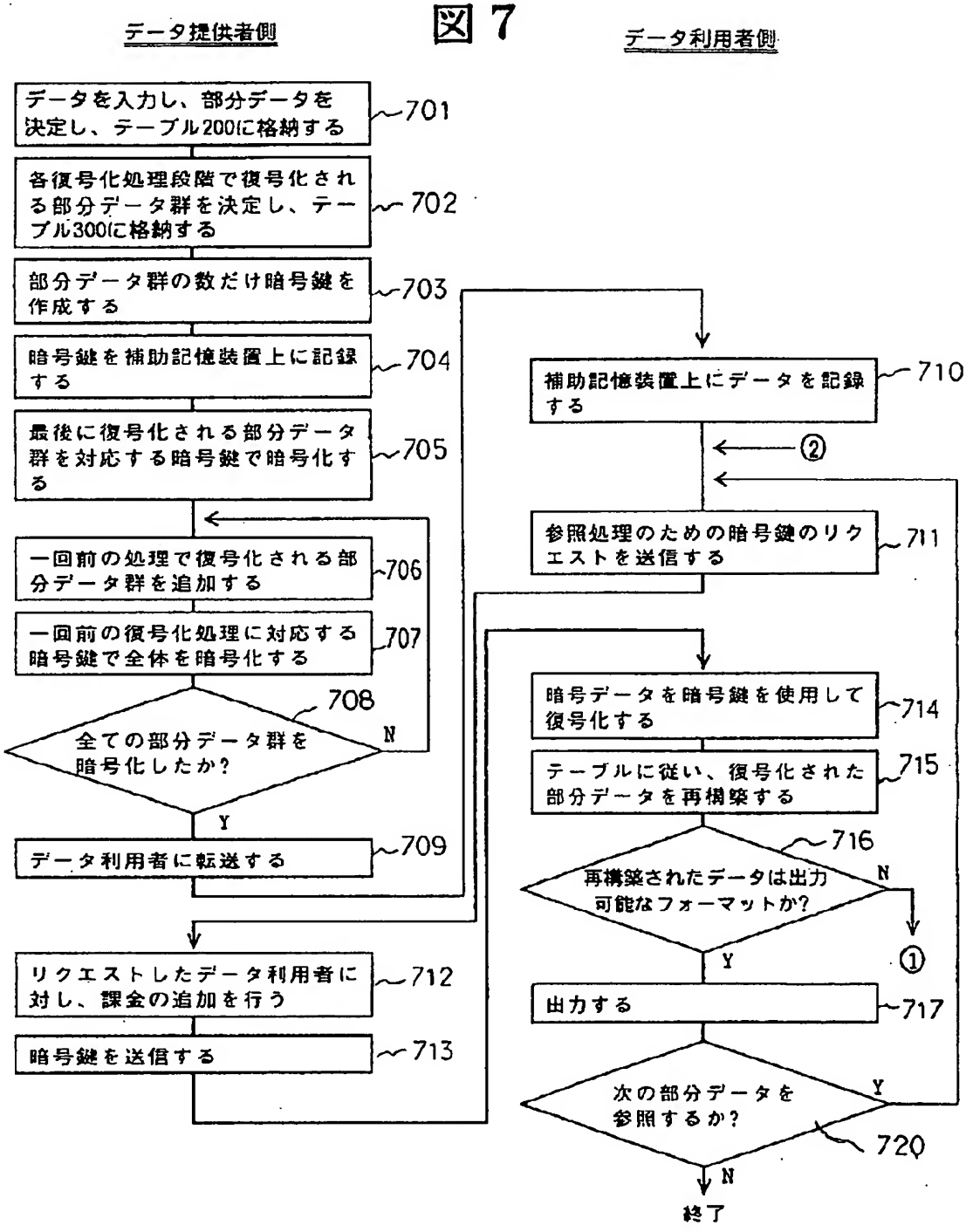
【図９】

図９



【図７】

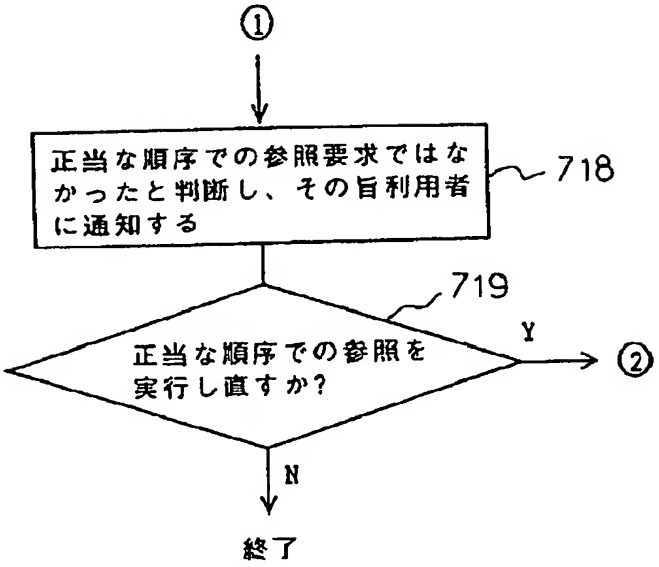
図７


データ提供者側
データ利用者側
データを入力し、部分データを決定し、テーブル200に格納する
701
各復号化処理段階で復号化される部分データ群を決定し、テーブル300に格納する
702
部分データ群の数だけ暗号鍵を作成する
703
暗号鍵を補助記憶装置上に記録する
704
最後に復号化される部分データ群を対応する暗号鍵で暗号化する
705
一回前の処理で復号化される部分データ群を追加する
706
一回前の復号化処理に対応する暗号鍵で全体を暗号化する
707
全ての部分データ群を暗号化したか?
708
N
Y
データ利用者に転送する
709
リクエストしたデータ利用者に対し、課金の追加を行う
712
暗号鍵を送信する
713
補助記憶装置上にデータを記録する
710
②
参照処理のための暗号鍵のリクエストを送信する
711
暗号データを暗号鍵を使用して復号化する
714
テーブルに従い、復号化された部分データを再構築する
715
再構築されたデータは出力可能なフォーマットか?
716
N
Y
①
出力する
717
次の部分データを参照するか?
720
Y
N
終了

【図８】

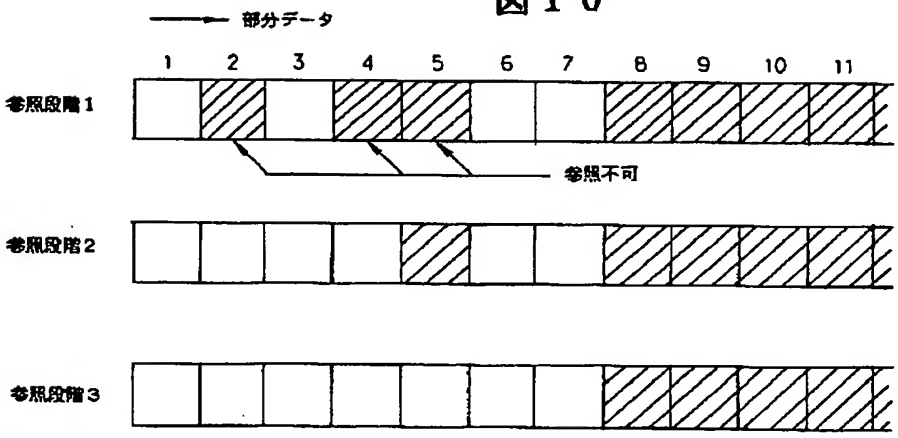
図８

データ利用者側



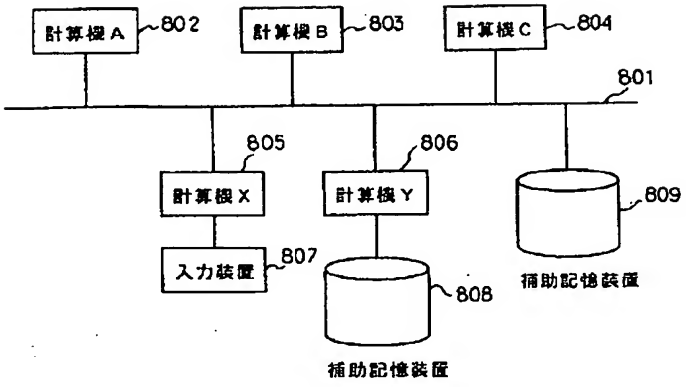
【図１０】

図１０



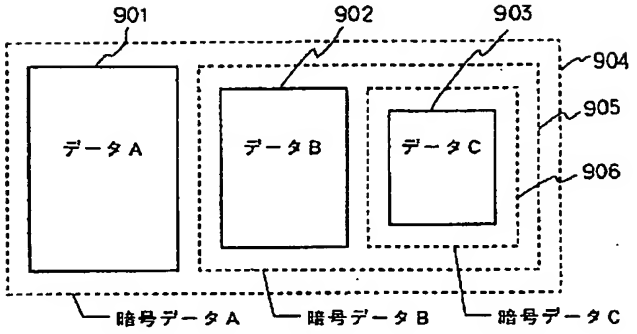
【図１１】

図１１



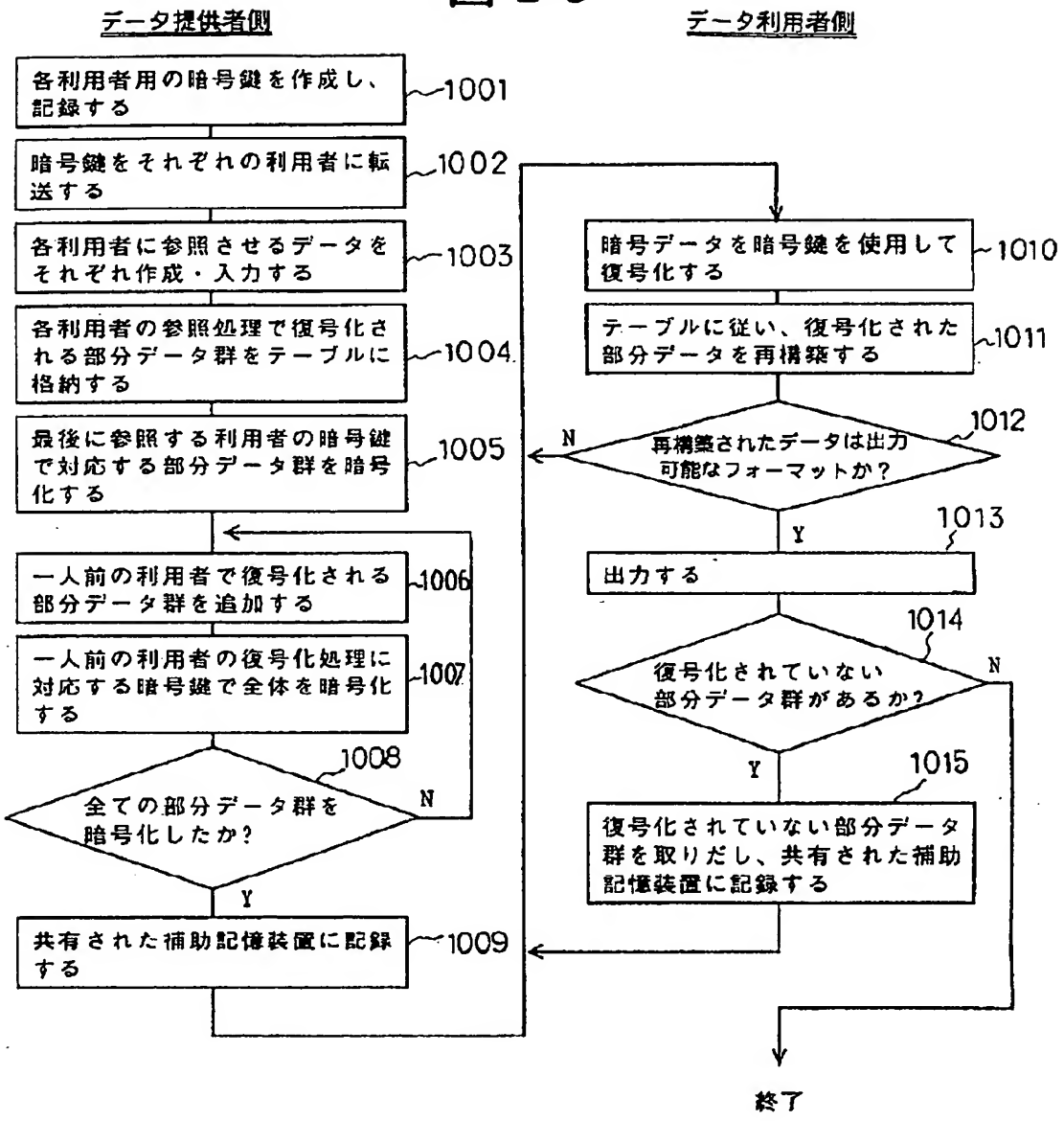
【図１２】

図１２



【図１３】

図１３


データ提供者側
データ利用者側
各利用者用の暗号鍵を作成し、記録する
1001
暗号鍵をそれぞれの利用者に転送する
1002
各利用者に参照させるデータをそれぞれ作成・入力する
1003
各利用者の参照処理で復号化される部分データ群をテーブルに格納する
1004
最後に参照する利用者の暗号鍵で対応する部分データ群を暗号化する
1005
一人前の利用者で復号化される部分データ群を追加する
1006
一人前の利用者の復号化処理に対応する暗号鍵で全体を暗号化する
1007
全ての部分データ群を暗号化したか?
1008
N
Y
共有された補助記憶装置に記録する
1009
暗号データを暗号鍵を使用して復号化する
1010
テーブルに従い、復号化された部分データを再構築する
1011
再構築されたデータは出力可能なフォーマットか?
1012
N
Y
出力する
1013
復号化されていない部分データ群があるか?
1014
N
Y
復号化されていない部分データ群を取りだし、共有された補助記憶装置に記録する
1015
終了

【公報種別】特許法第１７条の２の規定による補正の掲載
【部門区分】第７部門第３区分
【発行日】平成１３年７月１９日（２００１．７．１９）

【公開番号】特開２０００－１３８６６７（Ｐ２０００－１３８６６７Ａ）
【公開日】平成１２年５月１６日（２０００．５．１６）
【年通号数】公開特許公報１２－１３８７
【出願番号】特願平１１－３３８１４５
【国際特許分類第７版】
H04L 9/14
G06F 12/14 320
G09C 1/00 660
【ＦＩ】
H04L 9/00 641
G06F 12/14 320 B
G09C 1/00 660 D

【手続補正書】
【提出日】平成１２年７月７日（２０００．７．７）
【手続補正１】
【補正対象書類名】明細書
【補正対象項目名】発明の名称
【補正方法】変更
【補正内容】
【発明の名称】　回覧データ参照順の制御方法およびシステム並びに記録媒体
【手続補正２】
【補正対象書類名】明細書
【補正対象項目名】特許請求の範囲
【補正方法】変更
【補正内容】
【特許請求の範囲】
【請求項１】　回覧データ提供者側装置により提供される複数の部分データから成る回覧データ集合のうち、回覧データ利用者側装置の利用者が要求する参照権限順位の特定の部分データを当該利用者よりも上位の参照権限順位を有する全ての利用者が参照済みであることを条件に参照可能にする回覧データ参照順の制御方法であって、
回覧データ提供者側装置において複数の部分データから成る回覧データ集合に対して設定された参照権限順位数と同数の暗号鍵を生成または設定し、回覧データ利用者側装置に転送するステップと、
１つの参照権限順位に対応した特定の部分データに対し、次順位以降の参照権限の利用者で参照する全ての部分データをその参照権限順位に対応する暗号鍵で暗号化した暗号化部分データ集合を追加し、これら特定の部分データと暗号化部分データ集合とから成るデータ集合を当該参照権限順位に対応した暗号鍵で暗号化する処理を、参照権限順位数と同回数行ってデータ集合全体を暗号化し、この暗号化された回覧データ集合を記憶装置に格納するステップと、
回覧データ利用者側装置において、前記記憶装置に格納された回覧データ集合を回覧データ利用者からの要求に応じて取得し、当該利用者の参照権限順位に対応した暗号鍵によって対応する部分データを復号し、データ利用者が参照可能な形式で出力すると共に、復号した部分データ中に暗号化部分データが存在する場合には当該暗号化部分データを前記記憶装置に再格納するステップと、
を備えることを特徴とする回覧データ参照順の制御方法。
【請求項２】　回覧データ提供者側装置により提供される複数の部分データから成る回覧データ集合のうち、回覧データ利用者側装置の利用者が要求する参照権限順位の特定の部分データを当該利用者よりも上位の参照権限順位を有する全ての利用者が参照済みであることを条件に参照可能にする回覧データ参照順制御システムであって、
前記回覧データ提供者側装置は、複数の部分データから成る回覧データ集合に対して設定された参照権限順位数と同数の暗号鍵を生成または設定し、回覧データ利用者側装置に転送する暗号鍵生成手段と、
１つの参照権限順位に対応した特定の部分データに対し、次順位以降の参照権限の利用者で参照する全ての部分データをその参照権限順位に対応する暗号鍵で暗号化した暗号化部分データ集合を追加し、これら特定の部分データと暗号化部分データ集合とから成るデータ集合を当該参照権限順位に対応した暗号鍵で暗号化する処理を、参照権限順位数と同回数行ってデータ集合全体を暗号化し、この暗号化された回覧データ集合を記憶装置に格納する暗号化処理手段とを具備し、
前記回覧データ利用者側装置は、前記記憶装置に格納さ

れた回覧データ集合を回覧データ利用者からの要求に応じて取得し、当該利用者の参照権限順位に対応した暗号鍵によって対応する部分データを復号し、データ利用者が参照可能な形式で出力すると共に、復号した部分データ中に暗号化部分データが存在する場合には当該暗号化部分データを前記記憶装置に再格納する復号化処理手段を具備することを特徴とする回覧データ参照順制御システム。

【請求項３】　回覧データ提供者側装置により提供される複数の部分データから成る回覧データ集合のうち、回覧データ利用者側装置の利用者が要求する参照権限順位の特定の部分データを当該利用者よりも上位の参照権限順位を有する全ての利用者が参照済みであることを条件に参照可能にする回覧データ参照順の制御方法であって、

回覧データ提供者側装置において複数の部分データから成る回覧データ集合に対して設定された参照権限順位数と同数の暗号鍵を生成または設定し、回覧データ利用者側装置に転送するステップと、

最下位の参照権限順位に対応した特定の部分データを当該参照権限順位に対応する暗号鍵で暗号化し、該暗号化部分データに対し、１つ上位の参照権限順位の利用者が参照可能な部分データを追加し、これらの暗号化部分データと１つ上位の参照権限順位の部分データとを１つ上位の参照権限順位に対応する暗号鍵で暗号化する処理を、最上位の参照権限順位での部分データの暗号化が終了するまで繰返し、暗号化された回覧データ集合を記憶装置に格納するステップと、

前記回覧データ利用者側装置において、前記記憶装置に格納された回覧データ集合を回覧データ利用者からの要求に応じて取得し、当該利用者の参照権限順位に対応した暗号鍵によって対応する部分データを復号し、データ利用者が参照可能な形式で出力すると共に、復号した部分データ中に暗号化部分データが存在する場合には当該暗号化部分データを前記記憶装置に再格納するステップと、を備えることを特徴とする回覧データ参照順の制御方法。

【請求項４】　回覧データ提供者側装置により提供される複数の部分データから成る回覧データ集合のうち、回覧データ利用者側装置の利用者が要求する参照権限順位の特定の部分データを当該利用者よりも上位の参照権限順位を有する全ての利用者が参照済みであることを条件に参照可能にする回覧データ参照順制御システムであって、

前記回覧データ提供者側装置は、複数の部分データから成る回覧データ集合に対して設定された参照権限順位数と同数の暗号鍵を生成または設定し、回覧データ利用者側装置に転送する暗号鍵生成手段と、

最下位の参照権限順位に対応した特定の部分データを当該参照権限順位に対応する暗号鍵で暗号化し、該暗号化部分データに対し、１つ上位の参照権限順位の利用者が参照可能な部分データを追加し、これらの暗号化部分データと１つ上位の参照権限順位の部分データとを１つ上位の参照権限順位に対応する暗号鍵で暗号化する処理を、最上位の参照権限順位での部分データの暗号化が終了するまで繰返し、暗号化された回覧データ集合を記憶装置に格納する暗号化処理手段とを具備し、

前記回覧データ利用者側装置は、前記記憶装置に格納された回覧データ集合を回覧データ利用者からの要求に応じて取得し、当該利用者の参照権限順位に対応した暗号鍵によって対応する部分データを復号し、データ利用者が参照可能な形式で出力すると共に、復号した部分データ中に暗号化部分データが存在する場合には当該暗号化部分データを前記記憶装置に再格納する復号化処理手段を具備することを特徴とする回覧データ参照順制御システム。

【請求項５】　回覧データ提供者側装置により提供される複数の部分データから成る回覧データ集合のうち、回覧データ利用者側装置の利用者が要求する参照権限順位の特定の部分データを当該利用者よりも上位の参照権限順位を有する全ての利用者が参照済みであることを条件に参照可能にする回覧データ参照順の制御プログラムを記録した媒体であって、

回覧データ提供者側装置において複数の部分データから成る回覧データ集合に対して設定された参照権限順位数と同数の暗号鍵を生成または設定し、回覧データ利用者側装置に転送する処理と、

１つの参照権限順位に対応した特定の部分データに対し、次順位以降の参照権限の利用者で参照する全ての部分データをその参照権限順位に対応する暗号鍵で暗号化した暗号化部分データ集合を追加し、これら特定の部分データと暗号化部分データ集合とから成るデータ集合を当該参照権限順位に対応した暗号鍵で暗号化する処理を、参照権限順位数と同回数行ってデータ集合全体を暗号化し、この暗号化された回覧データ集合を記憶装置に格納する処理と、

回覧データ利用者側装置において、前記記憶装置に格納された回覧データ集合を回覧データ利用者からの要求に応じて取得し、当該利用者の参照権限順位に対応した暗号鍵によって対応する部分データを復号し、データ利用者が参照可能な形式で出力すると共に、復号した部分データ中に暗号化部分データが存在する場合には当該暗号化部分データを前記記憶装置に再格納する処理とを含むコンピュータが読み取り可能なプログラムが記録されていることを特徴とする記録媒体。

【請求項６】　回覧データ提供者側装置により提供される複数の部分データから成る回覧データ集合のうち、回覧データ利用者側装置の利用者が要求する参照権限順位の特定の部分データを当該利用者よりも上位の参照権限順位を有する全ての利用者が参照済みであることを条件

に参照可能にする回覧データ参照順の制御プログラムが記録されている媒体であって、
回覧データ提供者側装置において複数の部分データから成る回覧データ集合に対して設定された参照権限順位数と同数の暗号鍵を生成または設定し、回覧データ利用者側装置に転送する処理と、
最下位の参照権限順位に対応した特定の部分データを当該参照権限順位に対応する暗号鍵で暗号化し、該暗号化部分データに対し、１つ上位の参照権限順位の利用者が参照可能な部分データを追加し、これらの暗号化部分データと１つ上位の参照権限順位の部分データとを１つ上位の参照権限順位に対応する暗号鍵で暗号化する処理を、最上位の参照権限順位での部分データの暗号化が終了するまで繰返し、暗号化された回覧データ集合を記憶装置に格納する処理と、
前記回覧データ利用者側装置において、前記記憶装置に格納された回覧データ集合を回覧データ利用者からの要求に応じて取得し、当該利用者の参照権限順位に対応した暗号鍵によって対応する部分データを復号し、データ利用者が参照可能な形式で出力すると共に、復号した部分データ中に暗号化部分データが存在する場合には当該暗号化部分データを前記記憶装置に再格納する処理とを含むコンピュータが読み取り可能なプログラムが記録されていることを特徴とする記録媒体。

【手続補正３】
【補正対象書類名】明細書
【補正対象項目名】０００１
【補正方法】変更
【補正内容】
【０００１】
【発明の属する技術分野】本発明は、回覧データ提供者により提供される回覧データ集合を回覧データ利用者側で参照するシステムにおける回覧データの参照順の制御方法およびシステム並びに記録媒体に係り、特に、回覧データの利用者が要求する参照権限順位の特定の部分データを当該利用者よりも上位の参照権限順位を有する全ての利用者が参照済みであることを条件に参照可能にする回覧データ参照順の制御方法及びシステム並びに記録媒体に関する。